UNIVERSIDAD DE PANAMÁ

VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO

UNIVERSIDAD CARLOS III DE MADRID

MASTER EN GESTIÓN Y TECNOLOGIA DEL CONOCIMIENTO

Proyecto de Implementación de un Plan de Recuperación ante Desastres (DRP) para el Ministerio de Trabajo y Desarrollo Laboral

Sede Principal

Autores: María del C. Miranda M.

Cedula: 8-413-748

Tutores: Almudena Alcaide

Benjamín Ramos

TESIS PRESENTADA COMO UNO DE LOS REQUISITOS PARA OBTENER EL GRADO DE MASTER EN GESTIÓN Y TECNOLOGIA DEL CONOCIMIENTO

PANAMA REPÚBLICA DE PANAMA

- 2013 -

i-Índice

Capítulo 1

Capítulo 2

2.1 Estándares y Mejores Prácticas para la Planeación de la Continuidad del Negocio y Recuperación ante Desastres de Tecnología

2.1.a-Estándares ISO

2.1.b- Estándares BSI

2.2 Ejemplos de Plan de Recuperación ante Desastres

Capítulo 3

3.1 Desarrollo Plan de Recuperación ante Desastres del Ministerio de Trabajo y Desarrollo Laboral

3.1.1-Fase 1- Conocer la Organización

3.1.2- Fase 2- Evaluar los Riesgos y su Impacto en el Negocio

3.1.3- Fase 3- Análisis del Impacto al Negocio (BIA)

3.1.4- Fase 4- Plan de Recuperación ante desastres

Conclusiones

Bibliografía

Referencias a internet

Anexos

ii-Resumen

Este trabajo corresponde a nuestra tesis de grado, contiene información obtenida de una institución de gobierno de la República de Panamá; en el primer capítulo se proporciona información acerca de la situación actual de la institución en materia tecnológica, se definen los tipos de desastres naturales que se van a estudiar y se presenta la Metodología para desarrollar el plan de recuperación ante desastres.

El segundo capítulo hace una breve explicación de los estándares internacionales y mejores prácticas para la planeación de la continuidad del negocio y recuperación ante desastres así como casos de ejemplos.

En el tercer capítulo, se desarrolla el plan de recuperación como tal, se dan las recomendaciones pasos y procesos a seguir ante un evento natural.

iii-Abstract

This work relates to our thesis, contains information obtained from a government institution of the Republic of Panama, in the first chapter provides information about the current status of the institution in technology, defines the types of natural disasters be studied and presents the methodology to develop the disaster recovery plan.

The second chapter gives a brief explanation of international standards and best practices for planning business continuity and disaster recovery as well as case examples.

In the third chapter, we develop the recovery plan as such, recommendations are given steps and processes to be followed in a natural event.

iv- Indice de Cuadros y Figuras

Indice de Figuras **Pág**

Indice de Cuadros

Indice de Tablas

v-Palabras Clave

MITRADEL: Ministerio de Trabajo y Desarrollo Laboral

RPO: **(Recovery Point Objetive)** tiempo MAXIMO que la empresa está dispuesta a destinar para la recuperación de los datos.

RTO: **(Recovery Time Objetive)** es el tiempo establecido como mínimo para que las diferentes unidades de negocio puedan volver a su funcionamiento.

DRP: Es un conjunto de actividades y planes que se construyen con el objetivo de permitir que la empresa pueda retornar a una, condición de funcionamiento aceptable luego de haber ocurrido un evento de la naturaleza o desastre natural.

BCP: Es conocido como un proceso de crear un conjunto de planes y procedimientos dentro de la empresa con el objetivo de poder contar con un plan o procedimiento a seguir en caso de ocurrir un evento de la naturaleza.

KVA : El **voltamperio**, de símbolo **VA** es la unidad de la potencia aparente y de la potencia compleja de un aparato eléctrico. También se usa a menudo para la potencia reactiva, aunque la unidad recomendada para esta magnitud es el var (unidad). Dimensionalmente se corresponde con el vatio.

DATA CENTER: Centro de datos es donde se encuentran los recursos tecnológicos necesarios para que una empresa pueda procesar su información.

IDC: Data Center.

vi- PRESENTACIÓN DEL PROYECTO DE TESIS

La dependencia de la tecnología en el Estado Panameño se ha incrementado en los últimos años, dando como resultado un Gobierno más eficiente y competitivo. Ello conlleva a que sea mandatorio la confección e implementación de un Plan de Recuperación de Desastres en todas sus entidades y dependencias que utilicen las TIC's como herramienta en sus funciones cotidianas.

Como parte del continuo avance en las mejoras de procesos interno del Ministerio de Trabajo Y desarrollo Laboral, el presente documento busca servir de Modelo para la implantación de un plan de Recuperación de Desastres

dentro de la Entidad.

¿Por qué el plan de recuperación de desastres es esencial?

La Guía de Planeación de Recuperación de Desastres (The Disaster Recovery Guide, Open Directory Project) Recomienda que si un plan aún no existe, será necesario iniciar la preparación de la primer versión de dicho plan.

Para poder iniciar un proyecto de planeación por primera vez, el nivel superior de administración tendrá que recibir una propuesta.

Los proyectos importantes como la planeación de recuperación de desastres deberán ser aprobados en el nivel máximo para asegurar que el nivel adecuado de recursos y atención a la administración sea aplicado al proceso.

La propuesta deberá presentar las razones por las que se llevará a cabo el proyecto y podrá incluir todas o algunas de las siguientes:

• Dependencia en aumento por el negocio en años recientes en cuanto a producción computarizada y mecanismos de entrega de ventas, que ocasiona el aumento del riesgo de pérdida de servicios normales.

• Dependencia en aumento por el negocio en años recientes en cuanto al uso de sistemas computarizados de información.

• Consentimiento incrementado del impacto que un accidente serio podría provocar en el negocio.

• Necesidad de establecer un procedimiento formal a realizar cuando ocurra el desastre.

• Una tendencia hacia costos bajos o pérdidas derivadas de incidentes graves.

• Aumento de medidas de protección inadecuadas de tecnologías de información.

• Necesidad de desarrollar backups y estrategias de recuperación efectivas para mitigar el impacto de eventos disruptivos.

• Fracaso en el negocio provocado por incidentes disruptivos.

Básicamente, lo anterior es una lista de las razones más comunes por las que las organizaciones recurren a los planes de recuperación de desastres. Aquí se muestra de nuevo, cómo las empresas buscan adquirir uno de estos Planes, no necesariamente para prevenir un accidente, sino para recuperarse del impacto provocado por el desastre.

CAPITULO 1

INTRODUCCION PLAN DE RECUPERACION ANTE DESASTRES PARA EL MINISTERIO DE TRABAJO Y DESARROLLO LABORAL

1.1- INTRODUCCIÓN

¿Qué es un DRP?

Un DRP son, Procesos desarrollados con el objetivo de permitir a la empresa volver a condiciones estables, después de sufrir las afectaciones de un desastre natural. Esta básicamente orientado, a recuperar los servicios de tecnología.

¿Qué es un BCP?

El BCP, es más un proceso que se desarrolla de forma Global, dentro de la organización, (véase figura 1) ya que enmarca todos los planes o procedimientos que permiten garantizar la continuidad del negocio luego de ocurrido un desastre natural.

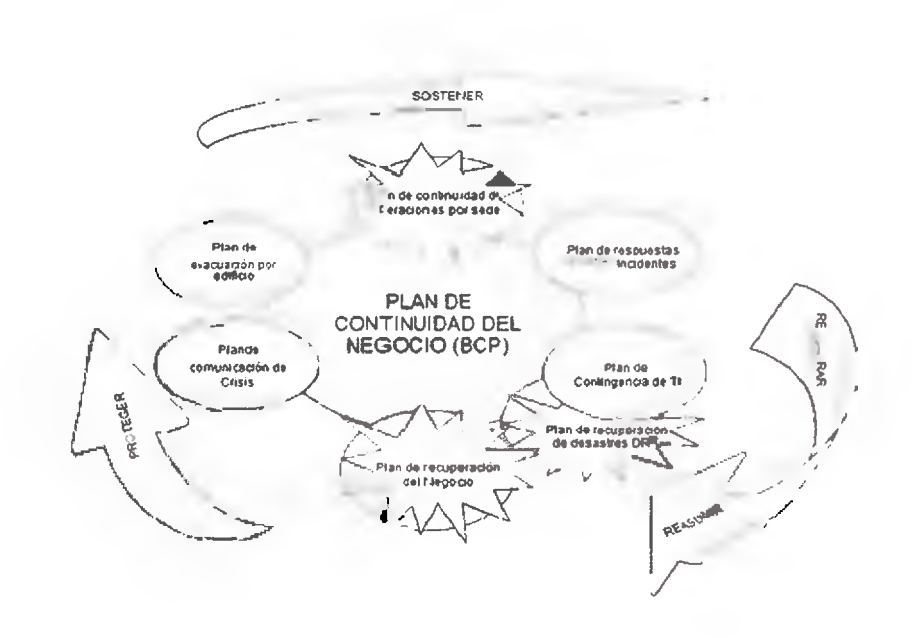


Figura 1- Plan de Continuidad del Negocio (BCP)

Un Plan de Recuperación ante desastres ,viene siendo parte del plan global de continuidad del negocio, es la estrategia que se seguirá para restablecer los servicios de TI (Hardware y Software) después de haber sufrido una afectación por una catástrofe natural, epidemiológica, falla masiva, daño premeditado, ataque de cualquier tipo el cual atente contra la continuidad del negocio.

Objetivo

Establecer el conjunto de estrategias, procedimientos, roles y responsabilidades requeridos, para reanudar los servicios de tecnología del Ministerio de Trabajo y Desarrollo Laboral, en caso de la ocurrencia de un evento de desastre que afecte la plataforma tecnológica.

1.2- Situación Actual del Ministerio de Trabajo y Desarrollo Laboral

El Ministerio de Trabajo y Desarrollo laboral es la institución encargada de regular la actividad Obrero Patronal en nuestro país.

Objetivos del Ministerio de Trabajo y Desarrollo Laboral:

Proyectar, promover, regular, administrar y ejecutar el sistema de administración del trabajo, estableciendo con el Órgano Ejecutivo, la Política Nacional Laboral, así como los Proyectos y Programas de Desarrollo Laboral del Estado, conforme con la Constitución Política, Leyes y Convenios Internacionales ratificados por Panamá; contribuyendo al Desarrollo Humano con Justicia Social, el Fomento del Diálogo Social Tripartito, el Trabajo Decente, la Promoción del Empleo digno en Igualdad de Género, la Protección de la Salud y Seguridad del Trabajador, particularmente de los sectores vulnerables como son, las Personas con Discapacidad y los Menores de Edad y Adolescentes Trabajadores.

OBJETIVO ESTRATÉGICOS

- Mejorar las capacidades del talento humano del Ministerio, a través de la capacitación permanente, brindándoles programas de incentivos a los colaboradores.
- Mejorar los procedimientos administrativos y funcionales de la Institución.
- Promover la excelencia en la atención de los clientes internos y externos, mediante el establecimiento de una cultura de mejoramiento continuo.

- Incorporar un programa de renovación permanente de la tecnología, con la adquisición de nuevos equipos informáticos de punta, que contribuyan a sistematizar las funciones del Ministerio de Trabajo y Desarrollo Laboral.

- Promover e incentivar la inserción laboral de las personas con discapacidad y el desarrollo de programas y proyectos de generación de empleo para grupos vulnerables, que coadyuven a disminuir la tasa de desempleo en el país.

- Fomentar los empleos productivos basados en competencias laborales y la inserción en el mercado de trabajo con igualdad de oportunidades para todos los trabajadores ciudadanos más vulnerables del país, a través de políticas laborales y de diálogo social.

- Establecer los mecanismos de control y supervisión, que garanticen el cumplimiento de las legislaciones y normas vigentes en el país, en cuanto a la seguridad laboral por parte de las empresas y trabajadores.

"ÁREAS ESTRATÉGICAS DEL MINISTERIO

- *Administración*

- *Planificación*

- *Capacitación*

- *Trabajo y Empleo*

- *Investigación y Observatorio Laboral*

- *Innovación Tecnológica*" [2]

Como podemos observar, el ministerio tiene entre sus objetivos y estrategias, ofrecer un servicio tecnológicamente innovador a todos los ciudadanos de la República de Panamá, es por esto que se hace necesario contar con un Plan de recuperación ante desastres robusto y que cumpla con las expectativas requeridas.

Por ser el ministerio un ente mediador entre trabajadores y empleadores, es común que ocurran eventos de reuniones entre sindicatos y empleadores, en las instalaciones del ministerio poniendo esto en riesgo las instalaciones y los equipos tecnológicos.

En ese sentido, entonces, el ministerio afronta los riesgos de desastres naturales y riesgos por ataques, sabotaje etc.

Actualmente, el ministerio de trabajo se encuentra ubicado en Plaza Edison, Avenida Ricardo J. Alfaro, utilizando los pisos:

Planta Baja

Piso 5

El centro de cómputo se encuentra ubicado en el piso 5, oficina 25 y 26.

El ministerio de trabajo esta fisicamente localizado en la vía Ricardo J. Alfaro, una de las principales vías de la ciudad de Panamá.

Es un edificio de 5 pisos en donde se encuentran ubicadas otras instituciones del estado y oficinas privadas.

Figura 2. Plaza Edison. Localización del Ministerio de trabajo y Desarrollo laboral en la ciudad de Panamá

En el anexo 2 se puede observar el plano arquitectónico completo del ministerio en donde se ve la ubicación física del data center del ministerio de trabajo y desarrollo laboral.

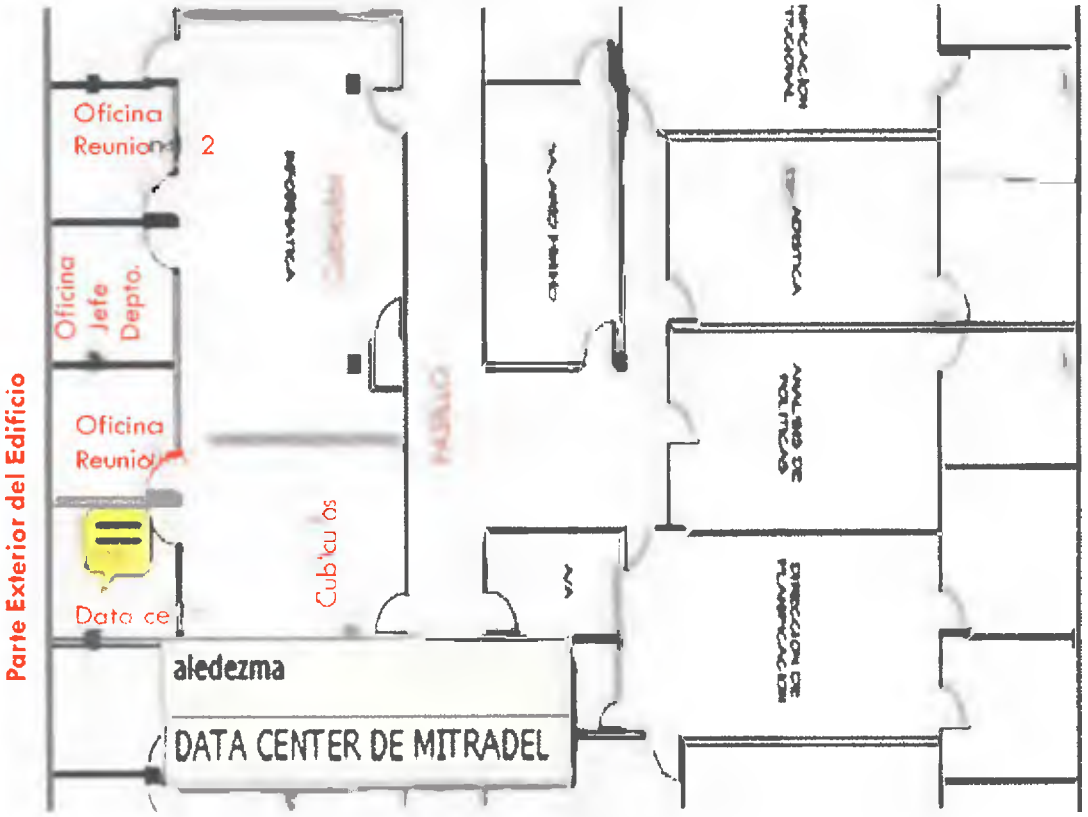


FIGURA 3. Extracto- Plano Arquitectónico Ministerio de Trabajo y Desarrollo Laboral

Como se muestra en la figura 3, actualmente el data center está ubicado dentro de una oficina de la Dirección de Informática.

EL data center cuenta con piso falso, una unidad de batería de 15 KVA, corriente limpia solo para los equipos del datacenter. (Ver Anexo 3).

Riesgos:

- El centro de cómputo se encuentra ubicado a escasos 20 metros del pasillo en donde transitan los visitantes que acuden día a día al ministerio.
- El centro de cómputo(Data Center) está dentro de las oficinas del departamento de informática
- Igualmente se encuentra en una habitación con ventana, la cual da hacia la parte de afuera del edificio, por ende está expuesto a sabotaje o daños por tormentas con fuertes vientos y lluvia.

En el presente anteproyecto, nos vamos a enfocar a los posibles desastres naturales, que puedan provocar daños a las instalaciones del edificio donde se encuentran las instalaciones tecnológicas del ministerio.

- Tormentas eléctricas
- Tornados

1.3– Desastres Naturales

Los desastres Naturales son fuertes e intensos cambios que ocurren a personas, bienes, servicios y medio ambiente. Mismos eventos que pueden sobrepasar la capacidad de respuesta del área que resultó afectada.

Entre estos tenemos:

a. *"Sismos/Terremotos.- Son los movimientos de la corteza terrestre que generan deformaciones intensas en las rocas del interior de la tierra, acumulando energía que súbitamente es liberada en forma de ondas que sacuden la superficie terrestre.*

b. *Maremotos/Tsunamis.- Movimiento de la corteza terrestre en el fondo del océano, formando y propagando olas de gran altura.*

c. *Erupciones Volcánicas.- Es el paso del material (magma), cenizas y gases del interior de la tierra a la superficie.*

d. *Deslizamiento de Tierras.- Que ocurren como resultado de cambios súbitos o graduales de la composición, estructura, hidrología o vegetación de un terreno en declive o pendiente:*

e. *Derrumbes.- Es la caída de una franja de terreno que pierde su estabilidad o la destrucción de una estructura construida por el hombre.*

f. *Aludes.- Masa de nieve que se desplaza pendiente abajo.*

g. *Aluviones.- Flujos de grandes volúmenes de lodo, agua, hielo, roces, originados por la ruptura de una laguna o deslizamiento de un nevado.*

h. *Golpe de agua o Huaycos.- Desprendimientos de lodo y rocas debido a precipitaciones pluviales, se presenta como un golpe de agua lodosa que se desliza a gran velocidad por quebradas secas y de poco caudal arrastrando piedras y troncos.*

i. *Inundaciones.- Invasión lenta o violenta de aguas de río, lagunas o lagos, debido a fuertes precipitaciones fluviales o rupturas de embalses, causando daños considerables. Se pueden presentar en forma lenta o gradual en llanuras y de forma violenta o súbita en regiones montañosas de alta pendiente.*

ı. *Tormentas.- Fenómenos atmosféricos producidos por descargas eléctricas en la atmósfera.*

j. *Granizadas.- Precipitación de agua en forma de gotas sólidas de hielo.*

k. *Tornados.- Vientos huracanados que se producen en forma giratoria a grandes velocidades.*

l. *Huracanes.- Son vientos que sobrepasan más 24 Km. /h como consecuencia de la interacción del aire caliente y húmedo que viene del océano Pacífico con el aire frío ".[5]*

1.3.1- Riesgos a los que está sometido el Ministerio de Trabajo y Desarrollo laboral

El ministerio de Trabajo como todas las instituciones de nuestro país tienen el riesgo latente de sufrir cualquier catástrofe natural que tenga como resultado, el no poder prestar el servicio que ofrece de forma continúa. A continuación se detallan:

- Desastres Naturales

-Tornado

- Terremoto

- Inundación

- Tormentas Eléctricas

Desastres creados por el Hombre

- Protestas que culminen con destrozos de equipos electrónicos

- Terrorismo

- Acceso no autorizado a los equipos informáticos

"Según las estadísticas disponibles, la República de Panamá es un país con una incidencia e impactos de desastres menores en comparación con el resto de Centroamérica; sin embargo, el país no está exento de ellos. Las poblaciones vulnerables, en su gran mayoría, se expanden hacia áreas de amenazas reconocidas por estudios técnicos de especialistas. El concepto de vulnerabilidad ante desastres socio-naturales toma amplio interés.

Con una población de aproximadamente 36.8% en condición de pobreza, incluyendo la pobreza urbana, la gente se vio obligada a concentrarse en áreas altamente

vulnerables (como los corregimientos de San Miguelito, Chorrillo, Calidonia, Juan Díaz, Alcalde Díaz, entre otras). Estas zonas se asocian a patrones de desarrollo urbano espontáneo, que no respetan las normas de construcción y que han adquirido hábitos de consumo poco higiénicos (acumulación de basura en fuentes de agua, basureros clandestinos en cualquier esquina de la ciudad, etc.). Las ciudades de Panamá y Colón, y con certeza el resto de las ciudades del país, viven en un constante nivel de riesgo. El país presenta fallas geológicas activas importantes: Falla de Tonosí, Zona de Fractura de Panamá, Falla de Gatún, el cinturón deformado del norte de Panamá, entre otras. En caso de que se produzca un sismo fuerte, en particular los centros urbanos se verían seriamente afectados, con las secuelas de falta de servicios y control de enfermedades. Eventos como el terremoto que impactó a las provincias de Bocas del Toro y Chiriquí en 1991; el paso del huracán Mitch en fase de tormenta tropical cerca de las costas panameñas en la provincia de Darién en 1998; los movimientos sísmicos de Chiriquí de 2001 y en Colón en el 2003; las trombas marinas avistadas en el área de la Bahía de Panamá en el 2002 y en agosto del 2003; las graves inundaciones del 17 de septiembre de 2004 en la capital, que dejaron un saldo de 16 víctimas mortales, 13.011 afectados y 1.405 damnificados, son eventos que evidenciaron que eran necesarias la preparación y participación comunitaria para enfrentar los impactos ocasionados por el impacto de amenazas naturales en este país".[1]

1.4-Objetivos específicos

- ✓ Recuperar la plataforma tecnológica que soporta los servicios críticos del Ministerio de Trabajo y Desarrollo Laboral.
- ✓ Definir los elementos y procedimientos necesarios que le permitan al Ministerio de Trabajo y Desarrollo Laboral soportar la recuperación efectiva y eficiente de los sistemas y aplicaciones que se encuentran respaldados.

- ✓ Reducir los tiempos de recuperación mediante la estructuración de las acciones a seguir antes, durante y después del evento que se presente.
- ✓ Alinear los diferentes procedimientos de contingencia documentados en la Gerencia de área de Tecnología.
- ✓ Garantizar la operación de los aplicativos del ministerio
- ✓ Permitir que el sistema se replique en servidores espejos fuera del sitio
- ✓ Garantizar la durabilidad de los equipos, manteniendo una frontera entre la corriente eléctrica y los mismos, evitando con esto posibles daños por picos de corriente.

1.5-Metodología

En este punto vamos a definir una metodología que proporcione una secuencia definida de pasos para elaborar de manera sistemática un plan para la continuidad y recuperación ante desastres para el Ministerio de trabajo y desarrollo laboral con el objetivo de que el mismo garantice la continuidad del negocio del citado ministerio.

1.5.1- Mapa de Ruta para la Metodología

1.5.1.1- Fase 1 Conocer la Organización

En esta fase se busca establecer la necesidad de desarrollar el plan de continuidad en la organización, de tal manera que se comunique la importancia de realizar este plan, involuerando a los directivos y el personal de la empresa. De modo que es, importante: conocer previamente en términos generales, la naturaleza de la situación, en cuestión. Por tal motivo, es necesario investigar los antecedentes de la problemática a tratar; lo cual, permitirá identificar el medio ambiente y las áreas donde se desenvuelve el problema.

Esta Fase genera las siguientes tareas:

-Conocer el medio ambiente general

-Identificar la estructura organizacional de la empresa

- Definir la arquitectura de macro procesos

- Definir equipos de planificación y sus responsabilidades

-Definición de objetivos, alcance y escenarios del problema

-Concienciación y aprobación por parte de los directivos

1.5.1.2-Evaluar los Riesgos

En esta etapa se deben identificar las amenazas internas y externas, incluyendo concentraciones de riesgo, permitiendo controlar y priorizar para formar una base que establezca un programa de control y un plan de acción de gestión de riesgo, se deben

identificar las actividades de misión critica de la organización, sus dependencias y sus puntos de fallas, también el análisis de impacto y el efecto que se generaría en caso de la pérdida o interrupción de las actividades de misión crítica.

Actividades de esta etapa:

- Identificación de las funciones , servicios y recursos críticos del área
- Análisis , evaluación y diagnóstico de riesgos
- Control de riesgos
- Evaluación y diagnóstico del análisis de impacto del negocio

1.5.1.3 Análisis del impacto al Negocio (BIA)

En esta fase, se lleva a cabo un análisis que permite visualizar que procesos o áreas son las más críticas en el negocio. Permite poder priorizar sobre cuáles aplicativos son necesarios llevar a otro sitio y cuales pueden mantenerse.

Esta fase, es la más importante y es la que debe ser más concisa y concreta, de modo que debe orientarse a presentar los resultados de los análisis realizados.

Actividades de esta fase:

- Desarrollar RTO (Objetivo de tiempo de recuperación)
- Desarrollar RPO (Punto de recuperación)
- Graficar Resultados

El **RTO (Recovery Time Objetive)** es el tiempo máximo que la compañía está dispuesta a destinar para la recuperación de los datos al haber pasado por un evento de pérdida de datos ya sea por desastre natural o alguna otra causa.

El **RPO (Recovery Point Objetive)** Nos indica la cantidad de datos máximo que se puede perder y que se acepta como tolerable ante la ocurrencia de un desastre natural o alguna otra causa.

1.5.1.4- Plan de Recuperación ante Desastres

En esta fase, se determinan los recursos mínimos para trabajar en el centro alterno, se describen las estrategias y se formalizan los procedimientos de reanudación y recuperación. Así mismo, se definen los procedimientos de notificación y escalamiento de emergencias y los criterios y procedimientos de activación de los planes de contingencia.

Actividades de esta fase:

- Diseñar estrategias de continuidad de la organización
- Presentar el análisis costo / Beneficio de las estrategias de continuidad
- Negociación y firma de contratos con los proveedores de servicios
- Adquisición de infraestructura de TIC's
- Preparación de sitio alterno
- Definir los procedimientos de recuperación

CAPITULO 2

ESTÁNDARES Y MEJORES PRÁCTICAS PARA LA PLANEACIÓN DE LA CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN ANTE DESASTRES DE TECNOLOGÍA

2.2- ESTÁNDARES Y MEJORES PRÁCTICAS PARA LA PLANEACIÓN DE LA CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN ANTE DESASTRES DE TECNOLOGÍA

Las normas, estándares y mejores prácticas para la planeación de la continuidad del negocio y recuperación ante desastres de Tecnología, tienen como objetivo establecer Medidas y patrones técnicos de administración y organización de las Tecnologías de la Información y de las Comunicaciones TIC´s de todo el personal comprometido en el Uso de los servicios informáticos proporcionados por la Unidad de Informática del Ministerio de Trabajo y Desarrollo Laboral.

A continuación un breve paso por las mismas:

2.2.1-Estándares

En el siguiente cuadro se presenta un resumen de los estándares internacionales orientados a la construcción de un plan de recuperación ante desastres, para todo tipo de compañía, el cual les permite volver a su estado normal y seguir ofreciendo el servicio, cualquiera que este sea.

Cuadro 1- Estándares

Tomado de: http://www.iso.org/iso/catalogue_detail?csnumber=44374

Estándar	Descripción
BS 25999-1:2006	*"Sirve como orientación para la implementación de un plan de continuidad de negocio"*
BS 25999-2:2007	*"Corresponde a los requisitos para implementar el plan y la certificación y auditoría del mismo."*
Estándares ISO/PAS	
ISO / IEC 27031:2011:	*"Describe los conceptos y principios de la tecnología de información y comunicación (TIC), la preparación para la continuidad del negocio, y proporciona un marco de métodos y procesos para identificar y especificar todos los aspectos (por ejemplo, los criterios de rendimiento, diseño y ejecución) para mejorar la preparación de la organización de las TIC para garantizar la continuidad del negocio. El ámbito de aplicación de la norma ISO / IEC 27031:2011 abarca todos los eventos e incidentes (incluidos los relacionados con la seguridad) que podrían tener un impacto en la infraestructura de las TIC y los sistemas. Se incluye y amplía las prácticas de manejo de incidentes de seguridad de información y la gestión y planificación de las TIC y los servicios de preparación."*
ISO / IEC 27001:2005:	*"Especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Información de Seguridad documentado de gestión en el contexto de los riesgos de negocio de la organización en general. Especifica los requisitos para la aplicación de controles de seguridad adaptados a las necesidades de organizaciones individuales o partes de los mismos. El estándar ISO/IEC 27001:2005 está diseñada para garantizar la selección de controles de seguridad adecuados y proporcionales que proteger los activos de información y dar confianza a las partes interesadas."*

ISO / PAS 22399:2007	*"Proporciona orientación general para una organización - las organizaciones privadas, gubernamentales y no gubernamentales - para desarrollar sus propios criterios de rendimiento específicos para la preparación de incidentes y la continuidad de trabajo y el diseño de un sistema de gestión apropiado. Proporciona una base para la comprensión, desarrollo e implementación de la continuidad de las operaciones y servicios dentro de una organización y para proporcionar la confianza en los negocios, la comunidad, los clientes, que responde en primer lugar, y de organización interacciones. También permite a la organización medir su capacidad de recuperación de una manera consistente y reconocida."*
ISO / IEC 27001:2005	*"Cubre todos los tipos de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro). ISO / IEC 27001:2005 especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Información de Seguridad documentado de gestión en el contexto de los riesgos de negocio de la organización en general. Especifica los requisitos para la aplicación de controles de seguridad adaptados a las necesidades de organizaciones individuales o partes de los mismos. El estándar ISO/IEC 27001:2005 está diseñada para garantizar la selección de controles de seguridad adecuados y proporcionales que proteger los activos de información y dar confianza a las partes interesadas."*

ISO / IEC 27031:2011	*"Describe los conceptos y principios de la tecnología de información y comunicación (TIC), la preparación para la continuidad del negocio, y proporciona un marco de métodos y procesos para identificar y especificar todos los aspectos (por ejemplo, los criterios de rendimiento, diseño y ejecución) para mejorar la preparación de la organización de las TIC para garantizar la continuidad del negocio. Se aplica a cualquier organización (privada, gubernamental y no gubernamental, independientemente de su tamaño) el desarrollo de su preparación para las TIC para el programa de continuidad del negocio (iRBC), y que requieren de sus servicios TIC / infraestructuras para estar listos para apoyar las operaciones del negocio en caso de salir eventos e incidentes e interrupciones relacionadas, que podrían afectar a la continuidad (incluida la seguridad) de las funciones críticas del negocio. También permite una organización para medir parámetros de rendimiento que se correlacionan con su iRBC de una manera consistente y reconocida. El ámbito de aplicación de la norma ISO / IEC 27031:2011 abarca todos los eventos e incidentes (incluidos los relacionados con la seguridad) que podrían tener un impacto en la infraestructura de las TIC y los sistemas. Se incluye y amplía las prácticas de manejo de incidentes de seguridad de información y la gestión y planificación de las TIC y los servicios de preparación."*

2.2.2- Mejores Prácticas

"Un acercamiento a "las mejores prácticas" significa la búsqueda de ideas y experiencias que han funcionado con aquellos que emprendieron actividades similares en el pasado y se decide cuál de esas prácticas son relevantes con la situación actual de la que partimos.

"Las mejores prácticas" no se refieren a "re-inventar la rueda", sino que es el aprendizaje a través de otros, con implementaciones que han sido desarrolladas para que funcionen correctamente". [3]

Por mejores prácticas entendemos un conjunto de actividades que han rendido un excelente resultado en un determinado contexto y se espera, que en contextos similares, rindan similares resultados.

Las organizaciones están cada vez más dependientes de la Tecnología de Información para dar soporte y hacer eficientes sus procesos de negocio con el objetivo de llenar las necesidades de los clientes y de la organización.

Paralelo a esto, la innovación tecnológica, calidad y valor de las nuevas tecnologías, siguen en incremento, de modo que se hace necesario que las organizaciones de TI tomen un enfoque orientado al negocio y al servicio en lugar de un enfoque centrado en la tecnología.

En este sentido para apoyar a las empresas en la construcción de Planes de Recuperación ante desastres naturales, existen mejores prácticas ya definidas y específicas por desastre natural.

En el siguiente cuadro se presentan las principales normas internacionales enfocadas a las mejores prácticas, definidas , probadas y afinadas para que sean utilizadas por las empresas al construir sus DRP's.

Cuadro 2- Mejores Prácticas

Mejores Prácticas	Descripción
ISO 17799/27002	*"ISO 27001 y 27002 proporcionan un marco eficaz para la organización de las actividades de seguridad y la garantía de que los recursos críticos están identificados, los riesgos se entiende, existen políticas adecuadas y los controles administrativos y técnicos están en su lugar. Este marco puede servir no sólo como una forma efectiva para construir y mantener un programa de seguridad, sino que también proporcionan los elementos necesarios para lograr el cumplimiento del creciente conjunto de normas de regulación de los contratos, como el Payment Card Data Security Standard y regulaciones estatales y federales, como la Información de Portabilidad y Responsabilidad, Gramm Leach Bliley, MA 201 CMR 17, y 603a Nevada".*[6]
COBIT	*"COBIT (Control Objectives for Information and related Technology) es el marco aceptado internacionalmente como una buena práctica para el control de la información, TI y los riesgos que conllevan. COBIT se utiliza para implementar el gobierno de IT y mejorar los controles de IT. Contiene objetivos de control, directivas de aseguramiento, medidas de desempeño y resultados, factores críticos de éxito y modelos de madurez. Para ayudar a las organizaciones a satisfacer con éxito los desafíos de los negocios actualmente, el IT Governance Institute® (ITGI) ha publicado la versión de COBIT® 4.1 COBIT es un framework de Gobierno de TI y un conjunto de herramientas de soporte para el gobierno de T.I. que les permite a los gerentes cubrir la brecha entre los requerimientos de control, los aspectos técnicos y riesgos de negocio. COBIT hace posible el desarrollo de una política clara y las buenas prácticas para los controles de T.I. a través de las organizaciones. COBIT enfatiza en la conformidad a regulaciones, ayuda a las organizaciones a incrementar el valor alcanzado desde la TI, permite el alineamiento y simplifica la implementación de la estructura COBIT. La última versión, COBIT® 4.1, enfatiza el cumplimiento normativo, ayuda a las organizaciones a incrementar el valor de T.I., apoya el alineamiento con el negocio y simplifica la implantación de COBIT. Esta versión no invalida el trabajo efectuado con las versiones anteriores del COBIT, sino que puede ser empleado para mejorar el trabajo previo. Cuando importantes actividades son planeadas para iniciativas de Gobierno de TI, o cuando se prevé la revisión de la estructura de control de la empresa, es recomendable empezar con la más reciente versión de COBIT".*[7]

ITIL	*"Marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI) de alta calidad. ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir de guía para que abarque toda infraestructura, desarrollo y operaciones de TI. Actualmente en Version 3".* [8]

2.2.3- Estándares VS Mejores Prácticas (Ventajas y Desventajas)

	Estándares, Buenas Practicas y Metodologías	Ventajas	Desventajas
Estándares	ISO 27001	Orientada a la Gestión de la Seguridad de la Información	Contempla parcialmente el tema de Continuidad del Negocio y Recuperación antes desastres de TI.
	ISO 24762	Guía para la provisión de servicios de recuperación de desastres como parte de la gestión de la continuidad del negocio.	Actualmente en desarrollo
	ISO 20000	Orientada a la Gestión de Servicios de TI	No Contempla el tema de recuperación ante desastres de TI en la continuidad del negocio
	BS 25999	Orientada a la gestión de la continuidad del negocio	Contempla parcialmente el tema de recuperación ante desastres de TI.
	NFPA 75	Orientada a la Protección contra incendios y la continuidad del negocio.	Contempla parcialmente el tema de Recuperación ante desastres de TI
	NIST SP 800-34	Guía para la planeación de contingencias en los sistemas de TI	Contempla parcialmente el tema de continuidad del Negocio.
Buenas Prácticas	ISO 17799/27002	Guía de buenas prácticas que describe los objetivos de control y controles en la administración de la seguridad de la información	Contempla parcialmente el tema de Recuperación ante desastres de TI en la continuidad del negocio.

	ISO 27005	Establece las directrices para la gestión del riesgo en la seguridad de la Información.	Contempla parcialmente el tema de recuperación ante desastres de TI.
	BS 25777	Guía de buenas prácticas que establece un marco para crear y mejorar un sistema de gestión de continuidad de servicios en los sistemas de TI.	Contempla parcialmente el tema de continuidad del negocio, se usa el estándar BS 25999 como complemento.
	COBIT	Brinda un marco de trabajo para la medición y monitoreo del desempeño de las tecnologías de información, definiendo las actividades de TI	Contempla la mayoría de los procesos relacionados con la continuidad del servicio, no tiene un enfoque integrado de todo el proceso.
	ITIL	Guía de prácticas destinadas a facilitar la entrega de servicios de TI de alta calidad abarcando la infraestructura, desarrollo y operaciones de TI.	Contempla la mayoría de los procesos relacionados con continuidad del servicio, no tiene un enfoque integrado de todo el proceso.
	COSO	Identifica los factores que causan Informes financieros fraudulentos y hace recomendaciones para reducir su incidencia.	No contempla el tema de recuperación ante desastres de TI en la continuidad del negocio.

Figura 4. Ventajas y Desventajas de los estándares, buenas prácticas y metodologías para emprender un modelo de gestión para la Planeación de la continuidad del Negocio y Recuperación ante Desastres.

3- Ejemplos de Plan de Recuperación ante desastres

A continuación mencionamos, Planes de recuperación ante desastres construidos para empresas existentes:

Resumen: Ejemplo 1

Lugar: Universidad de Puerto Rico Humacao

Año: Marzo 2007

Propósito: Este documento es el plan de recuperación de desastres para la Universidad de Puerto Rico en Humacao del departamento de Sistemas de Información Computación y Comunicación. La información contenida es una guía en la que se establecen las normas y los procedimientos que se utilizarán en caso de emergencia. El empleo de éstas, Capacitarán a la administración Universitaria y el personal técnico del SICC a responder asertivamente en caso de ocurrir un evento que destruya todas o parte de la las Facilidades del centro de cómputos de la UPR en Humacao. Además para reducir el Impacto negativo de eventos que puedan afectar a los Sistemas de Información, Computación y Comunicación de la UPRH.

Enfoque:

- Amenaza de Bomba
- Huracanes
- Tormentas , inundaciones
- Huelga

- Fuego
- Falta de electricidad

Ver Anexo 5 Plan de Recuperación de Desastres para la Universidad de Humacao Puerto Rico

Resumen: Ejemplo 2

Lugar: Banco de México, Continuidad operativa de la DGOBC del Banco de México

Fecha: Septiembre 2011

URL: http://www.cemla.org/old/actividades/2011/2011-09-SistematizacionBC/2011-09-SistematizacionBC-12.pdf

Propósito: Recuperar en el menor tiempo posible los servicios del banco, que todas las áreas del banco tengan un nivel de responsabilidad dentro del proceso de recuperación, lo que se logra integrando a el equipo en el proceso.

Enfoque:

- Terremotos,
- Inundaciones
- Situaciones humanas: huelga, acontecimientos políticos, pandemias, errores humanos, sabotajes

Ver Anexo 6 Continuidad Operativa en la Dirección General de Operaciones de Banca Central Banco de México

CAPITULO 3

DESARROLLO DEL PLAN DE RECUPERACIÓN ANTE DESASTRES NATURALES PARA EL MINISTERIO DE TRABAJO Y DESARROLLO LABORAL

3.1- DESARROLLO DEL PLAN DE RECUPERACIÓN ANTE DESASTRES NATURALES PARA EL MINISTERIO DE TRABAJO Y DESARROLLO LABORAL.

3.1.1-Fase 1 Conocer el ambiente de la Organización

En esta fase se llevan a cabo tareas que tienen como objetivo concienciar los miembros de la organización, igualmente plasmar los sistemas con los que se cuenta y su nivel de importancia o prioridad.

-Conocer el medio ambiente general

El ministerio de trabajo Desarrollo Laboral, es un ministerio con 40 años de funcionamiento. La mayor parte del personal es personal de más de 30 años de servicio, orientados al servicio al cliente.

En la actual administración se ha hecho una labor titánica para montar tecnología de punta en el ministerio que permita optimizar los procesos y agilizar la atención a los ciudadanos. Esta labor fue tomada de muy buen agrado por los colaboradores lo que ha permitido implementar sistemas tanto en la sede principal como en sus distintas regionales.

El ministerio cuenta con 10 regionales, una en cada provincia y comarca. En la ciudad capital cuenta con 3 regionales que apoyan la labor de la sede principal.

Actualmente el ministerio cuenta con la siguiente documentación respecto a

Controles:

- Procedimiento de la Unidad de Informática

Aquí se detalla los pasos que se deben seguir para tener acceso a el departamento, pasos para realizar una solicitud de soporte, pasos y registro del acceso al data center.

Se ha identificado al jefe de la Unidad de Informática, como responsable de la publicación y ejecución de este plan de recuperación ante desastres.

-Identificar la estructura organizacional de la empresa:

ANEXO 4 Organigrama Actual del Ministerio

- Definir la arquitectura de macro procesos

A continuación las distintas direcciones que conforman el ministerio de trabajo y desarrollo laboral:

Cuadro 3- Direcciones de Mitradel

Direcciones del Mitradel	Objetivo
Dirección Administrativa	*"Ejecutar las directrices emanadas de las autoridades superiores en materia de servicios administrativos de la institución, en lo referente a la ejecución, control de su presupuesto, de sus finanzas públicas, contabilidad, tesorería, compras y servicios generales, conforme a las funciones que se determinen en el Reglamento Orgánico del Ministerio y las normas de procedimientos generales aplicables".[2]*
Dirección de Trabajo	*"Organizaciones, dirección, coordinación y ejecución de las actividades técnicas en materia de relaciones de trabajo y soluciones de conflictos laborales.* *Que tiene como una de sus funciones principales, promover el diálogo social, como fundamento de la cultura laboral, que estimule la productividad y competitividad de los interlocutores sociales, así como un adecuado clima de relaciones laborales.* *Dirigir los servicios de conciliación y medicación, para la solución de los conflictos individuales y colectivos de trabajo".[2]*
Direttipat	*"- Prevenir y erradicar el trabajo infantil realizado por niños y niñas con edad por debajo de los 14 años.* *- Prevenir y combatir las peores formas de trabajo infantil de personas menores de 17 años.* *-Proteger el bienestar y derechos de las personas adolescentes trabajadoras entre las edades de 14 a 17 años.* *-Colaborar y participar en investigaciones y estudios de campo que sobre la materia realicen Organismos Nacionales y Extranjeros.*

	- Desarrollar programas para Erradicar las Peores Forma de Trabajo Infantil".[2]
Ipel	*"-Realizar seminarios, cursos, conferencias y charlas de capacitación sindical y laboral a nivel nacional e internacional.* *-Desarrollar y apoyar investigaciones socio-económicas.* *- Financiar para las organizaciones sociales legalmente constituidas, cursos y seminarios aprobados y autorizados por la Comisión de Educación Sindical y con sujeción a las partidas presupuestarias correspondientes.* *-Colaborar con otras instituciones públicas en el desarrollo de programas educativos y de capacitación para los obreros.* *- Proporcionar asistencia técnica a las organizaciones sociales".[2]*

- Definir equipos de planificación y sus responsabilidades

Para efectos del presente documento, el mismo está orientado a coordinar las tareas de recuperación ante desastres para la unidad de tecnología del ministerio.

Responsables:

- Director Administrativo (se encargará de aprobar el apoyo económico que el equipo que ejecuta, necesita para llevar a cabo el plan de forma exitosa).

- Jefe de Unidad de Informática (se encarga de reunir a los responsables por área. Coordina e informa las labores)

- Supervisor de soporte

- Supervisor Área de Base de datos y Programas

- Supervisor Área de infraestructura

-Definición de objetivos, alcance y escenarios del problema

Objetivos:

- Elaborar un procedimiento pasó a paso que permita restablecer los sistemas que utiliza el Ministerio de Trabajo y Desarrollo Laboral, para ofrecer el servicio al ciudadano Panameño.

Este plan debe lograr que los sistemas que utiliza el ministerio queden disponibles en el menor tiempo posible.

A continuación lista de las aplicaciones alta demanda que utiliza el ministerio:

Cuadro N. 4 Aplicaciones de Prioridad alta del Mitradel

UNIDAD ADMINISTRATIVA	SISTEMA		Prioridad
TESORERIA	Sistema de Pago de permisos de trabajo	internet	ALTA
Dir. de Empleo. Depto. de Migración Laboral	Sistema de Migración/Permisos de Trabajo	Oracle 10g	ALTA
Dir. de Empleo. Depto. de Mano de Obra	Pagina WEB y Bolsa de trabajo electrónica	Oracle 10g/Internet	ALTA

-Concienciación y aprobación por parte de los directivos

Para esta tarea se han llevado a cabo presentaciones ejecutivas en donde se les ha mostrado a las autoridades del ministerio, la importancia de contar con este plan, mostrándoles proyecciones de lo que ocurriría si ocurriese un evento natural en estos momentos. Todo esto con el objetivo de que ellos como autoridades, estén identificados con el proceso y permeen hacia sus equipos de trabajo la importancia y el nivel de compromiso que se necesita.

3.1.2-Fase 2 -Evaluar el Riesgos y su Impacto en el Negocio

Tareas de esta fase:

- **Identificación de las funciones , servicios y recursos críticos del área**

Cuadro 5-Identificación de Funciones, Servicios y Recursos Críticos del Área

UNIDAD ADMINISTRATIVA	SISTEMA	Área Dueña del Proceso
TESORERIA	Sistema de Pago de permisos de trabajo	Sistema Utilizado en la caja, Dirección administrativa, Departamento de tesorería.
Dir. De Empleo. Depto. De Migración Laboral	Sistema de Migración/Permisos de Trabajo	Sistema Utilizado en la Direc. De Empleo , Departamento de Migración
Dir. De Empleo. Depto. de Mano de Obra	Pagina WEB y Bolsa de trabajo electrónica	Sistema Utilizado en la Dirección de Empleo, Departamento de Mano de Obra/ Vía Internet de acceso a todos los ciudadanos

- **Análisis , evaluación y diagnóstico de riesgos**

El análisis, evaluación y diagnóstico de riesgos es el proceso de estimar la probabilidad de ocurrencia de un evento no esperado, el cual puede tener un nivel de severidad alto, teniendo esto consecuencias en la seguridad de las personas, medio ambiente y la comunidad.

Con este análisis se puede, entonces, desarrollar un plan de recuperación ante desastres que permita prevenir y minimizar los riesgos, atendiendo los eventos de forma efectiva.

"En una adecuada evaluación se debe considerar la naturaleza del riesgo, su facilidad de acceso o vía de contacto (posibilidad de exposición), la posibilidad de que ocurra y la magnitud de exposición y sus consecuencias, para de esta manera, definir medidas que permitan minimizar los impactos que se puedan generar. Dentro de este análisis se deben identificar los peligros asociados con los riesgos mencionados, entendiendo a estos peligros como el potencial de causar daño".[4]

- Metodología de Análisis de Riesgos por Colores:

Para desarrollar las actividades se llevó a cabo una investigación de las metodologías existentes para realizar el análisis de riesgo de forma más eficiente, encontrando esta metodología que vamos a utilizar a continuación.

"La metodología por colores cualitativa permite desarrollar análisis de amenazas y análisis de vulnerabilidad de Personas, recursos y sistemas y procesos, con el fin de determinar el nivel de riesgo a través de la Combinación de los elementos anteriores, con códigos de colores. Asimismo, es posible identificar una serie de observaciones que serán

la base para formular las acciones de Prevención, mitigación y respuesta que contemplan los planes de emergencia".[9]

Tabla 1- Calificación de las amenazas

Evento	Comportamiento	Color Asignado
Posible	Es aquel fenómeno que puede suceder o que es factible porque no existen razones históricas y científicas para decir que esto no sucederá.	
Probable	Es aquel fenómeno esperado del cual existen razones y argumentos técnicos científicos para creer que sucederá.	
Inminente	Es aquel fenómeno esperado que tiene alta probabilidad de ocurrir	

POSIBLE: NUNCA HA SUCEDIDO Color Verde.
PROBABLE: YA HA OCURRIDO Color Amarillo.
INMINENTE: EVIDENTE, DETECTABLE Color Rojo.

Tabla 2. Análisis de Amenazas para Mitradel

Amenaza	Interno	Externo	Descripción de la amenaza	Calificación	color
Tormentas Eléctricas		X	Eventos Atmosféricos que producen descargas eléctricas en la atmosfera.	INMINENTE	
Tornados		X	Son Vientos tipo huracanados que en forma giratoria, se producen a grandes velocidades.	PROBABLE	
Terremoto		X	Son los movimientos de la corteza terrestre que generan deformaciones intensas en las rocas del interior de la tierra, acumulando energía que súbitamente es liberada en forma de ondas que sacuden la superficie terrestre	POSIBLE	

Inundación	X	**Invasión lenta o violenta de aguas de río, lagunas o lagos, debido a fuertes lluvias o rupturas de embalses, y que causa una cantidad de daños.**	POSIBLE
Aludes o deslizamiento de tierras	X	**Cascadas de de tierra que se desplazan pendiente abajo.**	**POSIBLE**
Erupciones volcánicas	X	**Es el paso del material (magma), cenizas y gases del interior de la tierra a la superficie.**	POSIBLE

Elementos y Aspectos de Vulnerabilidad

Vulnerabilidades son características propias de un elemento o grupo de elementos expuestos a una amenaza, relacionada con su incapacidad física, económica, política o social de anticipar, resistir y recuperarse al daño sufrido cuando ocurre la amenaza. En la Tabla 3 se muestra los elementos y aspectos de Vulnerabilidad que vamos a analizar.

Tabla 3- Elementos y Aspectos de Vulnerabilidad

1- Persona	2-Recursos	3-Sistemas y Procesos
Gestión Organizacional	Suministros	Servicios
Capacitación y entrenamiento	Edificación	Sistemas Alternos
Características de seguridad	Equipos de IT	Recuperación

En el presente trabajo se analizarán los elementos Recursos, Sistemas y procesos. Debido a que el proyecto está delimitado a los equipos y servicios de Tecnología. Se estarán calificando de la siguiente manera: para un **SI** con 1(uno), para **PARCIAL** con 0.5(punto cinco) y para **NO** con 0(cero).

A continuación se presentan las tablas que desarrollan cada Aspecto de Vulnerabilidad para poder calificarlo y al final obtener como resultado el nivel de Vulnerabilidad que tiene la institución.

Tabla 4- Análisis de Vulnerabilidad de Equipos de IT

Punto A Evaluar	SI	NO	PARCIAL	Calificación	Observación
¿Existe un sistema de detección y/o monitoreo de la amenaza identificada?		X		0	
¿Existe una sistema de alarma en caso de emergencia?	X			1	
¿Existe un sistema de control o mitigación de la amenaza identificada?		X		0	
¿Existe un sistema de comunicaciones internas para la respuesta a emergencias?			X	0.5	
¿Existen medios de transporte para el apoyo logístico en una emergencia?	X			1	
¿Existe un programa de mantenimiento preventivo y correctivo para los equipos de emergencia?	X			1	REGULAR
Promedio				**0.58**	

Tabla 5- Análisis de Vulnerabilidad para Servicios

Punto A Evaluar	SI	NO	PARCIAL	Calificación	Observación
¿Se cuenta con suministro de energía permanente?	X			1	
¿Se cuenta con un servicio de comunicaciones internas?	X			1	
¿Se cuenta con procedimientos de contingencia documentados en las áreas de mano de obra, migración y caja?			X	0.5	
¿Se cuenta con papelería suficiente en caso de no contar con el servicio automatizado?	X			1	
¿Se cuenta con servicio de seguridad para custodio de las áreas expuestas, al momento de un	X			1	**BUENO**

desastre?					
Promedio:					**0.9**

Tabla 6- Análisis de Vulnerabilidad para Sistemas Alternos

Punto A Evaluar	SI	NO	PARCIAL	Calificación	Observación
¿Se cuenta con sistemas redundantes para la base de datos de Migración?		X		0	
¿Se cuenta con sistemas redundantes para acceso a internet?	\			1	
¿Se cuenta con sistema redundante de correo electrónico (Zimbra)?			x	0.5	
¿Se cuenta con sistemas redundantes para los equipos de comunicación de la sede principal?			X	0.5	
¿Se cuenta con sistema redundante para los equipos de Base de datos de aplicaciones y datos?		x		0	**REGULAR**
		Promedio			**0.4**

Tabla 7- Análisis de Vulnerabilidad para Procesos de Recuperación

Punto A Evaluar	SI	NO	PARCIAL	Calificación	Observación
¿Se tienen identificados los procesos vitales para el funcionamiento de su organización?		X		0	
¿Se cuenta con un plan de continuidad del negocio?		X		0	
¿Se cuenta con algún sistema de seguros para las integrantes de la organización?	X			1	
¿Se tienen aseguradas las edificaciones y los bienes en general para cada amenaza identificada, incluyendo los equipos tecnológicos?	X			1	

¿Se encuentra asegurada la información digital y análoga de la organización?	X	0	**REGULAR**
	Promedio:		**0.4**

Tabla 8-Interpretacion de Vulnerabilidad por cada elemento

Rango	Interpretacion	Color
0-1	ALTA	Rojo
1.01-2.00	MEDIA	Amarillo
2.01-3.00	BAJA	Verde

Tabla 9 Interpretación de la Vulnerabilidad por cada aspecto

Calificacion	Condicion
BUENO	Si el numero de respuestas se encuentra dentro del rango 0,68 a 1
REGULAR	Si el numero de respuestas se encuentra dentro del rango 0,34 a 0,67
MALO	Si el numero de respuestas se encuentra dentro del rango 0 a 0.33

En base a la tabla 8 y 9, procedemos a analizar los resultados:

Tabla 10- Resultados del Análisis de Vulnerabilidad

Aspectos	**Resultados**	**Nivel de Vulnerabilidad**
Recursos	Promedio (0.58)	ALTA
Sistemas y Procesos	Promedio(0.56)	ALTA

Se califica como **ALTA** la vulnerabilidad de que el Ministerio de Trabajo y Desarrollo Laboral, en su sede principal, pueda sufrir los efectos de un desastre natural, tormenta eléctrica o tornado,

- **Control de riesgos**

Riesgos: Posibles daños que pueden ocurrir a: la población, bienes, infraestructuras, medio ambiente, economía; por la ocurrencia de un desastre natural, que por su magnitud e impacto, hace que sea necesario contar con un proceso de gestión, que involucre áreas como el estado y la sociedad.

Utilizaremos, para interpretar los resultados las tablas 8 y 9 de la actividad anterior.

Tabla 11- Análisis de valores de Vulnerabilidad y Riesgo

			Sistemas y procesos							Nivel de Riesgo	
Amenaza	Calificación	Color	Recursos Equipos de IT	Color	Servicios	Sistemas Alternos	Recuperación	Promedio Sistemas y Procesos	Color	color	Interpretación
Desastres Naturales (Tormenta Eléctrica, Tornado)	Inminente		0.58		0.9	0.4	0.4	1.7			MEDIO

Los siguientes aspectos a considerar, presentados en la tabla 12, proporcionan una protección contra los riesgos descritos Minimizando su ocurrencia implementando los controles adecuados.

Tabla 12- Aspectos a considerar

Riesgo	los Mínimos a considerar
Tormenta Eléctrica Y Tornados	Fuentes Alternas de generación eléctrica :UPS's , plantas eléctricas
	Mantenimiento de las fuentes alternas de generación eléctrica
	Estado de la instalación eléctrica y capacidad eléctrica instalada
	Lámparas de emergencia
	Señalamiento iluminado de salidas y puertas de emergencia
	Soporte técnico de los equipos utilizados
	Pólizas de seguro vigentes
	Brigadas de atención ante situaciones de emergencia capacitación al personal

Conclusión de los análisis:

El Riesgo de que ocurran los eventos naturales, objeto de estudio, es de un nivel MEDIO. Lo cual no es muy alentador, puesto que el nivel de Vulnerabilidad salió ALTO. Esto nos da el soporte necesario para implementar este Plan de Recuperación ante desastres y que el mismo debe ponerse en práctica con urgencia notoria.

3.1.3-Fase 3 Análisis del Impacto al Negocio (BIA)

En esta fase vamos a desarrollar, el impacto del desastre en cada función crítica (Business Impact Analisys, BIA). Este análisis permite identificar los riesgos asociados a las funciones críticas de la organización y el impacto en una escala de tiempos que producirían esos riesgos. Esta información permite establecer prioridades a la hora de plantear la estrategia de recuperación. A la hora de realizar el BIA, se establecen prioridades como por ejemplo:

1. Evitar pérdidas de vida.

2. Reanudar las operaciones lo antes posible.

3. Proteger el medio ambiente.

4. Lograr las conexiones con los principales clientes y proveedores.

5. Mantener la confianza en la empresa.

El BIA implica determinar las labores y los recursos esenciales para respaldar la continuidad del negocio de MITRADEL (sede principal), su criticidad, su impacto para el negocio, sus RTOs (Recovery Time Objective - tiempo de recuperación objetivo),

RPOs (RecoveryPoint Objective - punto de recuperación objetivo) y

MTDs (Maximum Tolerable

A continuación se presenta tabla de los rangos de clasificación para el RTO y el RPO que puede soportar la institución. A este resultado se llego mediante entrevistas a niveles los Tácticos y Operativos de la institución.

Tabla 13- Rangos para clasificación

	Días	Puntaje
Rango 1	0-1	90.0
Rango 2	2-3	80.0
Rango 3	3-5	70.0

APLICACIÓN	UNIDAD ADMINISTRATIVA	SISTEMA	RTO	RPO
Sistema 1	TESORERÍA	Sistema de Pago de permisos de trabajo	**Rango 1/90,0**	**Rango 2/80,0**
Sistema 2	Dir. De Empleo. Depto. De Migración Laboral	Sistema de Migración/Permisos de Trabajo	**Rango 1/90,0**	**Rango 2/80,2**
Sistema 3	Dir. De Empleo. Depto. de Mano de Obra	Pagina WEB y Bolsa de trabajo electrónica	**Rango 2/80,0**	**Rango 2/80,2**

En el cuadro se puede apreciar, según el análisis realizado el nivel de tolerancia a las fallas que tienen las principales aplicaciones del Ministerio de Trabajo y Desarrollo Laboral. Para efectos del RPO las 3 aplicaciones manejan el mismo punto máximo de tiempo, y es que el ministerio le ofrece servicios de ciudadanos y no puede tener las aplicaciones fuera de servicio por más de 12 horas.

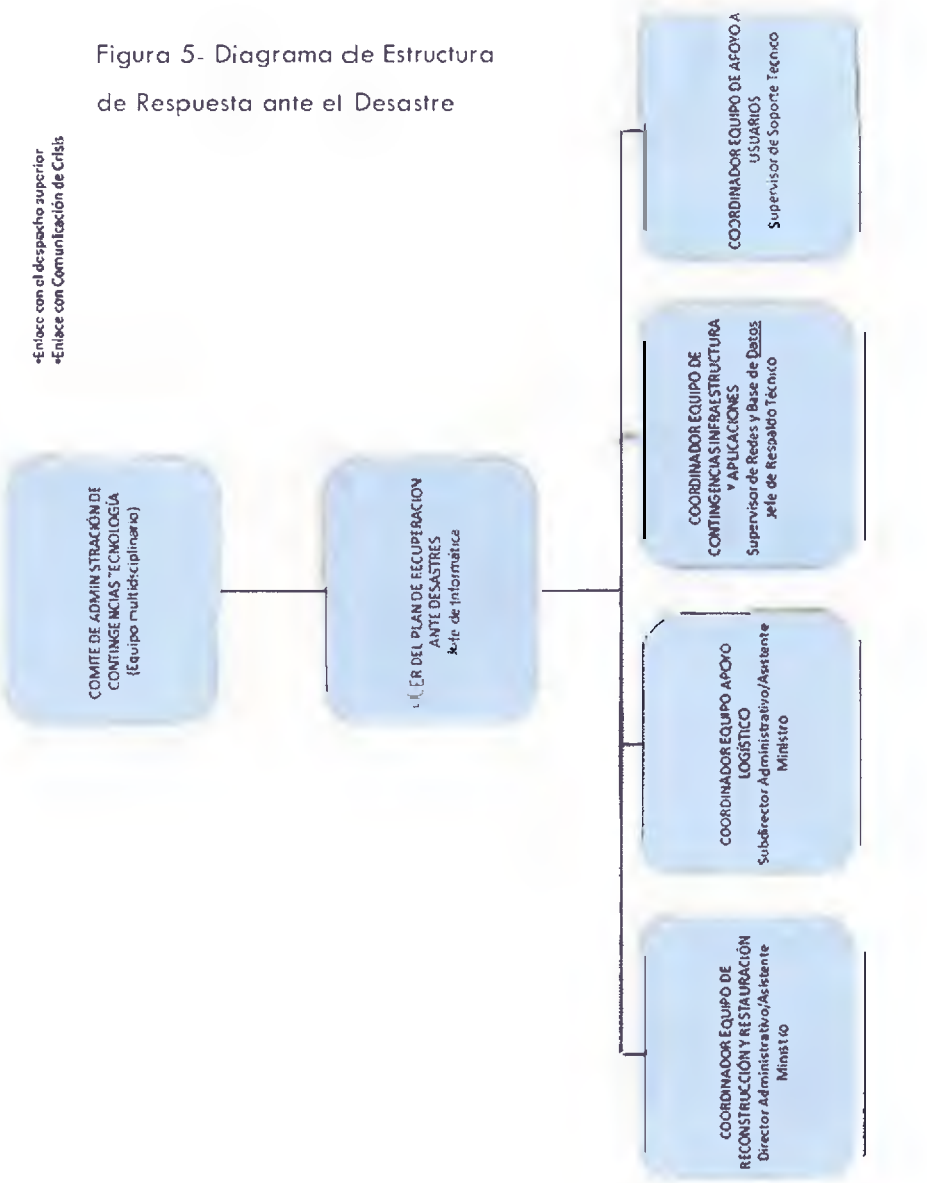
3.1.4-Fase 4 Plan de Recuperación ante desastres

- **Diseñar estrategias de continuidad de la organización**

El Ministerio de Trabajo y Desarrollo Laboral, debe contar con un sitio alterno de replicación de datos, tipo espejo. De modo que al momento de la ocurrencia de algún evento natural, los sistemas se tarden el tiempo definido en el RTO en estar nuevamente en línea.

Teniendo este punto como objetivo, entonces, debemos elaborar una estructura de Respuesta ante del desastre, de modo que cada persona sepa el orden de comunicación.

Figura 5- Diagrama de Estructura de Respuesta ante el Desastre



Definición de Roles:

Comité de Administración de Contingencias Tecnología

- Se encarga de planificar, ejecutar y comunicar las actividades del proceso de recuperación de forma que se logre el objetivo de volver a poner los sistemas

- Debe reunirse cada mes para revisar el proceso, agendar pruebas y hacer talleres de educación a todos los funcionarios del Ministerio a Nivel Nacional
- Debe contar con un presupuesto aprobado de $150,000.00 , el cual será utilizado para compra inmediata de equipos, con el objetivo de restaurar aplicaciones

Líder del Plan de Recuperación ante desastres

- Dirige, administra y coordina las labores que debe realizar el comité
- Velar por el cumplimiento de las funciones y las estrategias establecidas

Coordinadores

- Se encargan de ejecutar los procesos de recuperación definidos en sus áreas
- Comunica de manera efectiva las acciones a todos los directores de la institución
- Rinden cuenta el líder de comité, reportando estatus cada hora durante el desastre y durante la ejecución del proceso de recuperación
- Se encargan de contactar proveedores para ejecución de las tareas indicadas o documentadas
- Ejecutan las compras que se requieran de manera inmediata

-Presentar el análisis costo / Beneficio de las estrategias de continuidad

El análisis Costo/ Beneficio es el proceso de colocar cifras en dólares en los diferentes costos y beneficios de una actividad. AL utilizarlo podemos estimar el impacto financiero acumulado de lo que queremos lograr.

Tabla 14- Análisis Costo / Beneficio

Costos	$	Beneficios	$
Horas extras de personal de tecnología	5,000.00	Soporte durante los procesos críticos	5,000.00
Alimentación del personal técnico y de apoyo	2,000.00	Garantizar integridad del Personal	6,000.00
Transporte del personal	600	Garantizar integridad del Personal	10,000.00
Alquiler sitio alterno : incluye equipos, soporte, atención 24/7(mensual)	30,000.00	Seguridad de la información	100,000.00
Soporte de Base de datos 24/7(anual)	14,000.00	Apoyo de proveedores expertos en misiones criticas	38,400.00
Switches de comunicación	7,500.00	restablecimiento de comunicación en poco tiempo	4,500.00
Totales	59,100.00		163,900.00

-Negociación y firma de contratos con los proveedores de servicios

En la negociación y firma de los contratos con los proveedores, se debe tener en consideración que a manera de prevención se tienen contratos anuales y mensuales de servicio. Para efectos de que ocurra un evento, dichos contratos entran en vigencia de forma normal.

Tabla 15- Empresas proveedoras de servicios

Contratos de servicios Informátic...				
Empresa Contratada	**Aplicación/ Servicio**	**Contratante**	**Medio**	**Observaciones**
SSA SISTEMAS	Base de Datos	Mitra del	Licitación Publica	Lic. Publica Abreviada, 4 horas en portal PanamaCompras
Telecarrier	Hosting	Mitra del	Licitación Publica	Lic. Publica, para servicio de hosting de servidores mensual
HP Panamá	Equipos de comunic.	Mitra del	Licitación Publica	Lic. Publica Abreviada, 4 horas en portal PanamaCompras
Cable Onda Pma	Internet	Mitra del	Licitación Publica	Lic. Publica para servicio de internet, anual
Cable & Wirelles	Internet	Mitra del	Licitación Publica	Lic. Publica, para servicio de internet, anual
UPS DE PANAMA	DataCenter	Mitra del	Licitación Publica	Lic. Pública, Abreviada, 4 horas en portal Pma. Compras

Anexo: Ejemplos de los contratos de servicios.

-Adquisición de infraestructura de TIC's

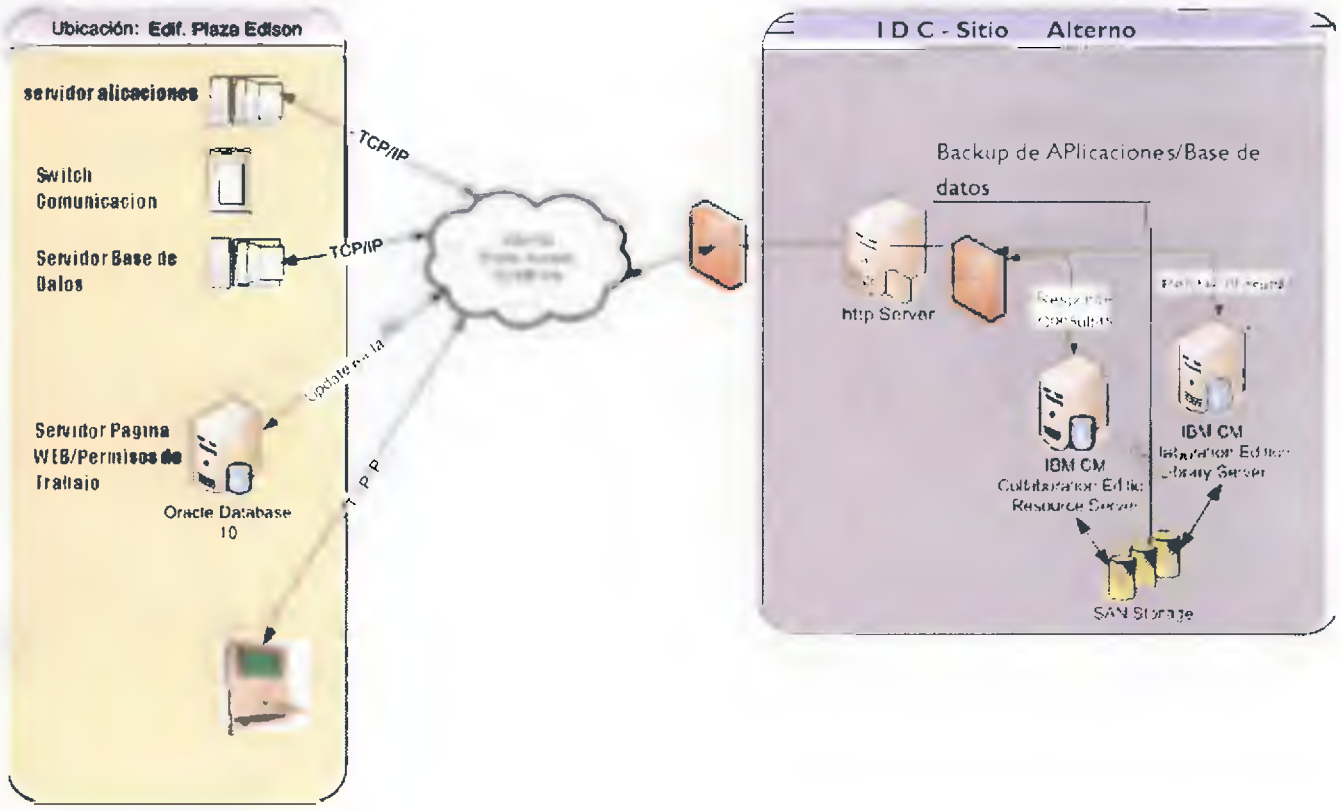
Para proceder con la adquisición de los equipos debemos proceder a tener un listado detallado de los mismos:

Figura 6- Adquisición de Equipos

Equipo para DATA CENTER (Reconstrucción)
UPS Liebert de 15 KVA Trifásico
1 Sistema de Control Ambiental Enfriado por Aire, Split Evaporador de 3 ton
1 Unidad Condensadora Liebert, Modelo PFH037A-YL3
Compresor
Porta filtro

- **Preparación de sitio alterno**

Figura 7- Diagrama propuesto de Sitio Alterno de Replicación para el Ministerio de Trabajo y Desarrollo Laboral



Este diagrama muestra, la infraestructura propuesta para sitio alterno del Ministerio de Trabajo y Desarrollo Laboral.

Sitio Alterno: IDC de Telecarrier

Ubicación: Clayton Tecno Parque

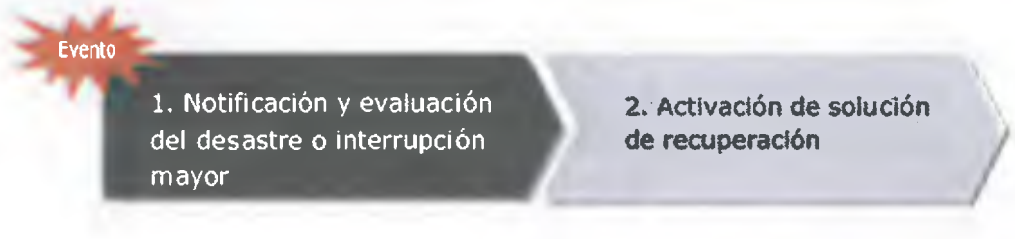
Piso 5, Jaula 70

El sistema tendrá la función Principal de ser un espejo de los servidores principales, ubicados en el data center de Mitradel, Servidores de Aplicación y Servidores de Base de datos, Pagina WEB y Base de datos de Permisos de Trabajo.

Actualmente, el Ministerio cuenta con un data Center equipado con los recursos mínimos para operar, permitiéndole al ministerio soportar todas las operaciones que se llevan a cabo en la institución. Ver ANEXO 8.

-Definir los procedimientos de recuperación

En esta actividad se busca detallar los procedimientos que debe seguir el personal para activar los planes de contingencia, activación de los equipos de trabajo, activación del sitio alterno etc.



Primero definimos un árbol de llamadas para que los equipos sepan a qué personas comunicar el evento:

Tabla 16- Árbol de Llamadas

NIVEL 0	NIVEL 1	NIVEL 2	NIVEL 3
Líder del Plan de recuperación ante desastres	▪ Coordinador equipo Apoyo Logístico ▪ Coordinador Equipo de	▪ Ministro(a) ▪ Vice Ministro ▪ Secretario General ▪ Coordinador de Equipo de Apoyo a usuarios	

Contingencia de Infraestructura, Comunicación y Aplicaciones		
▪ Coordinador Equipo de Reconstrucción y Restauración	▪ Jefe de Mantenimiento ▪ Jefe de Obras y Proyectos ▪ Jefe de Servicios Administrativos (Compra y Seguros)	

A continuación se describe el detalle de las actividades a ejecutar:

Tabla 17- Actividades a Ejecutar en el plan de recuperación

#	Actividad ¿Qué hacer?	Descripción ¿Cómo hacer?	Responsable
1. Notificación y Evaluación del desastre o interrupción mayor			
1.1	Notificar el desastre o interrupción mayor al Líder del plan de recuperación ante desastres.	Identifican la ocurrencia del desastre o incidente que genera la interrupción sobre la plataforma tecnológica y notifican el evento mediante los medios y el árbol de llamadas establecido. La notificación se debe realizar cuando se presenta alguno o varios de los siguientes escenarios: • No disponibilidad del centro de cómputo de Mitradel Sede Principal por desastres naturales. En la notificación, Se debe tener en cuenta que si el desastre es evidente, se debe notificar de acuerdo a las prioridades establecidas en los mecanismos de comunicación, sin embargo se debe dejar registro posterior de la notificación en el formato.	Operadores y Supervisores Coordinador Equipo Contingencia de Infraestructura, Comunicaciones y Aplicaciones Jefe de Mantenimiento
1.2	Evaluar el incidente / desastre en	Evaluar los daños considerando los siguientes elementos:	Líder del Plan de recuperación ante desastres

#	Actividad ¿Qué hacer?	Descripción ¿Cómo hacer?	Responsable
	forma preliminar	• Afectación del Centro de Cómputo • Afectación de la Plataforma tecnológica (Caracterizar el escenario de interrupción) • Tiempos estimados de solución (incluyendo tiempos de desplazamiento, solución y re-establecimiento de la operación). • Tiempo transcurrido desde la notificación del incidente hasta el momento de finalizar el diagnóstico. Tenga en cuenta en la evaluación, si es requerido, apoyarse en el coordinador de Reconstrucción y Restauración. Si se requiere convocar al Comité de Administración de Contingencias y Desastres, estableciendo un centro de comando en el IDC de Telecarrier.	Coordinador Equipo Contingencia de Infraestructura, Comunicaciones y Aplicaciones Coordinador de Reconstrucción y Restauración en caso de ser requerido.
2. Activación del desastre o interrupción mayor			
2.1	Establecer el Centro de Comando de Contingencias y Desastres	Instalar el Centro de Comando de Contingencias y Desastres en el IDC de Telecarrier Asegurar la disponibilidad del Centro de Comando de Contingencias y Desastres seleccionado, mediante la verificación de los siguientes aspectos: • Que no haya sido afectado por el mismo evento de desastre. • Que las rutas de acceso estén despejadas y el sitio sea accesible. • Que los medios de comunicación, voz y datos estén operando. • Que cuente con los recursos y servicios públicos necesarios	Líder del Plan de recuperación ante desastres

#	Actividad ¿Qué hacer?	Descripción ¿Cómo hacer?	Responsable
		En el caso que no cumpla con estas condiciones, se debe notificar al líder del plan de recuperación ante desastres para que active el centro de comandos alterno.	
2.2	Convocar al Comité	Convocar el Comité de Administración de Contingencias de Tecnología, informando la ubicación del Centro de Comando de Contingencias y Desastres.	Líder del Plan de recuperación ante desastres
2.3	Evaluar y activar el plan	El Líder del Plan de recuperación ante desastres reporta la evaluación inicial realizada del evento al Comité de Administración de Contingencias de Tecnología, quien tomará la decisión de activar o no el plan de recuperación ante desastres , teniendo en cuenta las siguientes consideraciones: a. Si es un desastre cuyo escenario de interrupción es conocido, y el tiempo de resolución total desde el momento en que se notificó la falla es menor al RTO de la plataforma, solicitar accionar los mecanismos de soporte y atención para solucionar el incidente. b. Si es un desastre cuyo escenario de interrupción es conocido y el tiempo de solución total desde el momento en que se notificó la falla puede tardar un tiempo superior al requerido para la plataforma, active la estrategia de recuperación en el Centro de Cómputo de Recuperación que corresponda. Si la decisión es no activar el plan de recuperación ante desastres, se deberá monitorear permanentemente la evolución del incidente, y evaluar nuevamente, en caso de que ocurran inconvenientes, si se activa o no el plan.	Comité de Administración de Contingencias de Tecnología
2.4	Notificar la activación de los planes / procedimientos	Notificar, de acuerdo a lo establecido en el árbol de llamadas, la activación del plan de recuperación ante desastres.	Líder del Plan de Contingencia y Recuperación ante Desastre

#	Actividad ¿Qué hacer?	Descripción ¿Cómo hacer?	Responsable
2.5	Activar Centro de Computo Alterno	De acuerdo al escenario que se haya identificado, activar la estrategia de recuperación que corresponda ,Esta activación contempla: • Comunicar la activación al Equipo de Contingencia de Infraestructura, Comunicaciones y Aplicaciones • Coordinar la ejecución de los procedimientos de recuperación, según el caso	Coordinador Equipo Contingencia de Infraestructura, Comunicaciones y Aplicaciones
2.6	Notificar el incidente o desastre al negocio	Suministrar información al negocio sobre el incidente o desastre ocurrido, teniendo en cuenta los siguientes aspectos: La información a proveer contiene: • Fecha y hora del reporte • Incidente presentado • Acciones tomadas • Acciones por desarrollar • Tiempo estimado de solución	Comité de Administración de Contingencias de Tecnología
2.7	Monitorear el incidente o desastre	En el caso en que las estrategias y procedimientos de recuperación hayan sido activados, se debe: • Verificar que la activación, alistamiento y disponibilidad de los centros de cómputo alternos se esté llevando a cabo de acuerdo a lo establecido en el plan. • Mantener contacto con los diferentes coordinadores de equipo. • Tomar decisiones sobre inconvenientes presentados en la activación de los procedimientos y las estrategias de recuperación. El Líder del Plan de recuperación ante desastres debe mantener una bitácora o trazabilidad de las decisiones tomadas por el Comité, apoyado en el	Comité de Administración de Contingencias de Tecnología

#	Actividad ¿Qué hacer?	Descripción ¿Cómo hacer?	Responsable
		Anexo 7: Registro de problemas y soluciones. En el caso en que las estrategias y procedimientos de contingencia y recuperación **NO** hayan sido activados, se debe: • Monitorear la situación y estar al tanto de las acciones que los coordinadores realizan para mitigar los incidentes presentados. Si el tiempo de solución esperado se extiende, el Comité debe evaluar nuevamente la necesidad de activación de las distintas estrategias de contingencia y recuperación. Por lo cual, se regresa a la **actividad 1.2 "Evaluar el incidente / desastre en forma preliminar".** Finalizado el procedimiento de recuperación, el líder del plan de recuperación ante desastres apoyado con los coordinadores de contingencia, formalizan la finalización del procedimiento de recuperación apoyado en el **Anexo 8: Finalización de la recuperación ante desastre o interrupción mayor**. Igualmente, el Comité de Administración de Contingencias de Tecnología deberá notificar al negocio la recuperación de la plataforma. La información a proveer contiene: • Fecha de inicio y fin del incidente • Incidente presentado • Acciones tomadas • Estado de la plataforma • Restricciones de la plataforma en contingencia.	
2.8	Iniciar el	Si el incidente ocasionó daños en el Centro de	Coordinador

#	Actividad ¿Qué hacer?	Descripción ¿Cómo hacer?	Responsable
	procedimiento de reconstrucción del Centro de Cómputo Principal	Cómputo Principal. Contactos con Proveedores de Servicios encargados de prestar el servicio tanto de instalación como de configuración de los equipos de computo en el data center.	Equipo de Reconstrucción y Restauración
2.9	Cierre del incidente o desastre	Una vez se hayan ejecutado los procedimientos relacionados con el incidente presentado, el Líder del Plan de Recuperación ante Desastres, deberá dar cierre del plan. En este caso se identificaran y documentaran las lecciones aprendidas del incidente, oportunidades de mejora sobre el DRP y las estrategias, y cualquier aspecto relevante para mejorar la efectividad del DRP.	Líder del Plan de Recuperación ante Desastres. Coordinador de preparación en Recuperación ante Desastres y Contingencias
	FIN		

CONCLUSIONES

Actualmente el gobierno de Panamá está invirtiendo millones de dólares, en infraestructura de tecnología para las instituciones, que ofrecen servicio a los ciudadanos panameños. Esto provoca que sea parte vital de los procesos definidos de la institución, contar con un Proceso de Recuperación ante desastres, correctamente documentado. Con el objetivo de salvaguardar la información de los ciudadanos que día a día realizan tramites en la institución. En ese sentido consideramos que se deben tener en cuenta las siguientes consideraciones:

- ✓ Se hace necesario ejecutar prácticas de este plan de recuperación ante desastres, para garantizar y afinar su funcionamiento.
- ✓ Un Plan disminuye la confusión durante un evento
- ✓ Un plan de Recuperación ante desastres, le permite a la institución ser Proactiva y no Reactiva
- ✓ Tomar las acciones correctivas cuando sea necesario
- ✓ Se deben establecer controles que mitiguen el riesgo
- ✓ Respuesta ordenada ante un desastre

BIBLIOGRAFÍA

[COBIT] COBIT aplicado para asegurar la continuidad de las operaciones.
http://www.isacamty.org.mx/archivo/213-COBIT_Aplicado_Para_Asegurar_Continuidad_Operaciones.pdf

[ACIS] Planes de recuperación ante desastres DRP
http://www.acis.org.co/fileadmin/Conferencias/DRP_BCP.pdf

Loney, Kevin; Theriault, Marlene. Oracle 9i Manual del administrator.
McGraw- Hill/Interamericana de España, S.A.U

Panadero, Enrique. La necesidad de implantación de un plan de continuidad de negocio.
Illera Manager Systems & Process Assurance
http://www.borrmart.es/articulo_redseguridad.php?id=564&numero=18

[SOLINGEST] http://www.solingest.com/blog/cluster-de-servidores-que-es-y-comofunciona

Curso Acelerado V 2.0, DRI The Institute for Continuity Management.https://www.drii.org/certification/professionalprac.php

H. Wold, Geoffrey. Disaster Recovery Planning Process.
http://www.drj.com/new2dr/w2_002.htm

Oracle Parallel Server Architecture.
http://technet.oracle.com/doc/windows/server.804/a55925/chap3.htm

REFERENCIAS DE INTERNET

[1] http://www.eird.org/perfiles-paises/perfiles/index.php/Panam%C3%A1

[2] http://www.mitradel.gob.pa

[3] http://www.ibit.org/dades/doc/1658_ca.pdf

[4] **metodologías de análisis de riesgo** documento soporte guía - fopae
www.fopae.gov.co/portal/.../A.3.4%20**Metodologias**%20AR.pdf

[5] http://www.monografias.com/trabajos12/ldesast.shtml

[6] http://en.wikipedia.org/wiki/iso/iec_27002

[7] http://www.isaca.org/knowledge_center/cobit/pages/overview.aspx

[8] http://www.itil-officialsite.com

[9] http://www.biblio-sepi.esimez.ipm.mx/sistemas/2010/Metodologia.....pdf

www.tele-carrier.com

www.sigweb.cl

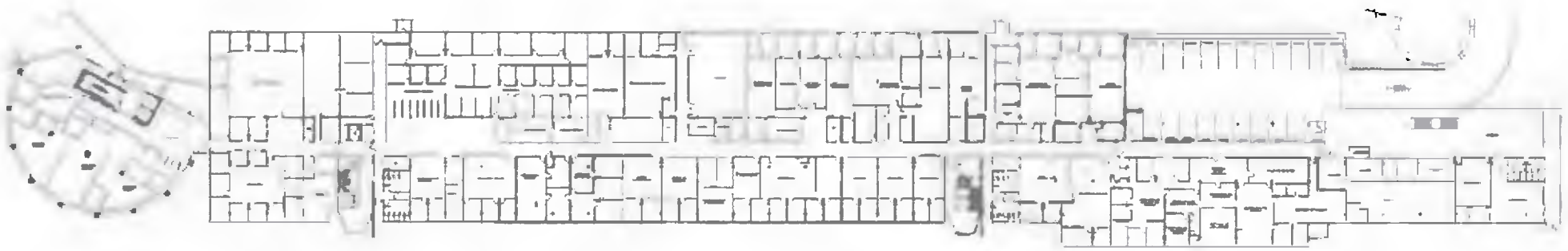
ANEXOS

ANEXO 1

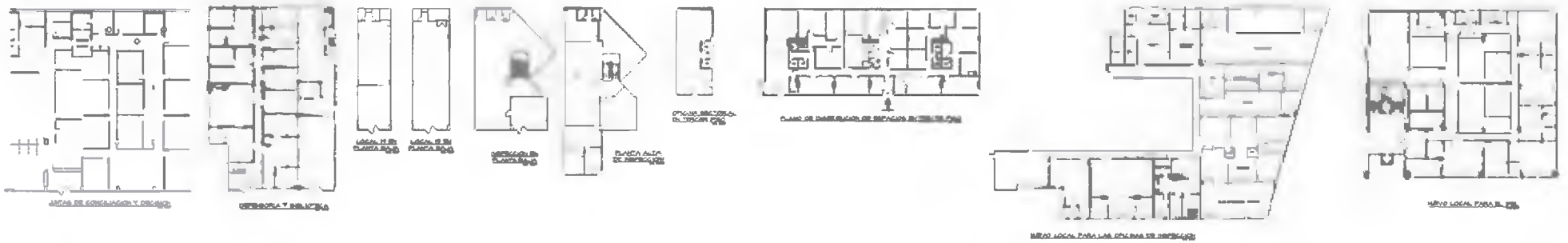
TORMENTAS ELECTRICAS, INUNDACIONES, DAÑOS A ESTRUCTURAS Y EDIFICIOS EN PANAMA

ANEXO 2

PLANO ARQUITECTONICO DE MITRADEL



PLANTA ARQUITECTONICA ACTUAL EN QUINTO PISO DE PLAZA EDISON



MINISTERIO DE TRABAJO Y DESARROLLO LABORAL
DIRECCIÓN DE PLANIFICACION
DEPARTAMENTO DE PLANIFICACION INSTITUCIONAL

PLANOS DEL MINISTERIO DE TRABAJO Y DESARROLLO LABORAL
EN PLAZA EDISON

SEPT. 2010

1 DE 1

ANEXO 3

DATA CENTER de MITRADEL


Piso Falso

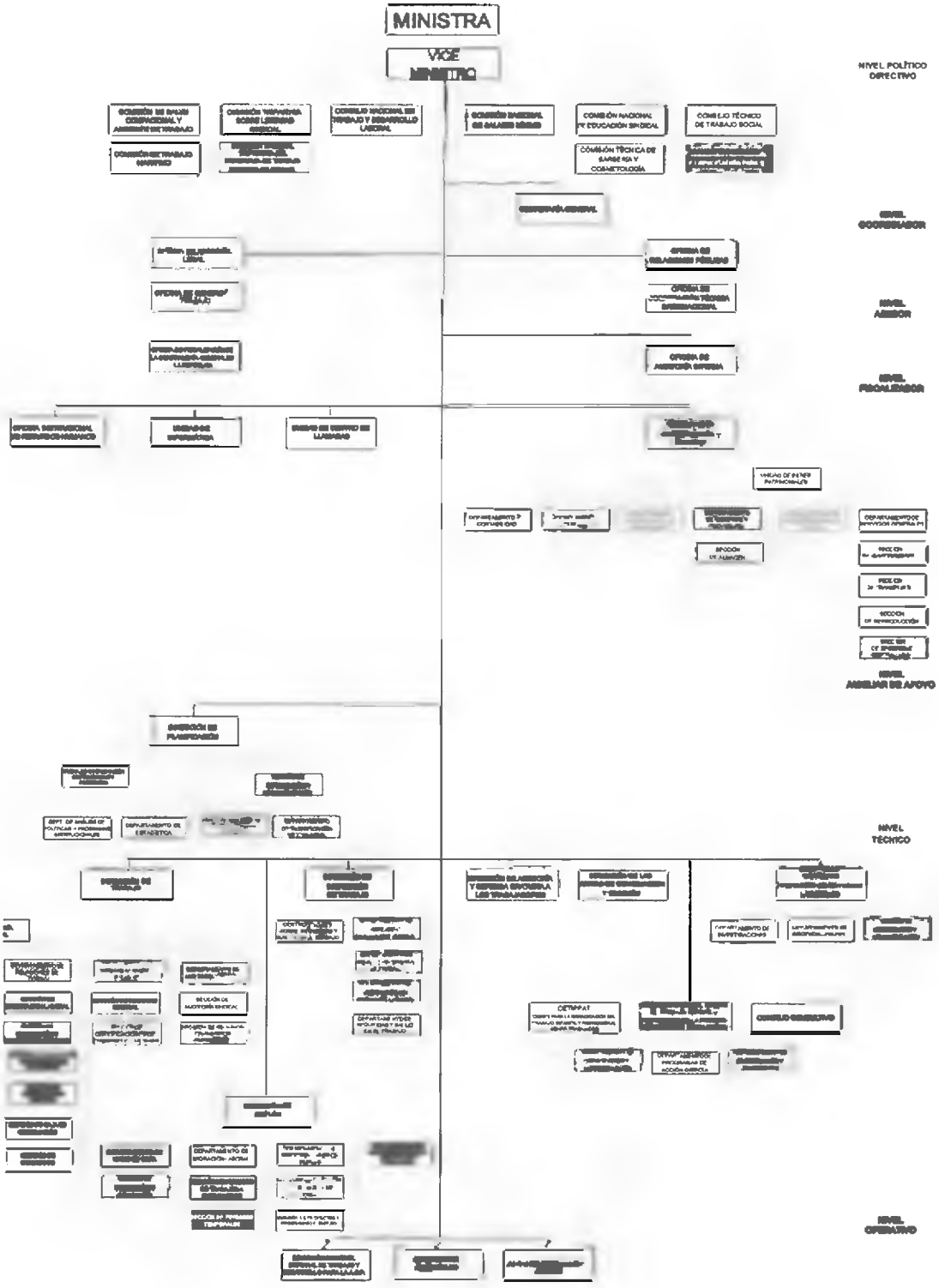
ANEXO 4

Organigrama Ministerio de Trabajo y Desarrollo Laboral

MINISTERIO DE TRABAJO Y DESARROLLO LABORAL

ESTRUCTURA ORGANIZATIVA

ACTUAL



AGOSTO - 2019

Anexo 5

Plan de Recuperación de Desastres para la Universidad de Humacao Puerto Rico

Universidad de Puerto Rico en Humacao
Oficina de Sistemas de Información, Computación y Comunicación

Plan de Recuperación de Desastres

Marzo 2007

Tabla de Contenido

1 Introducción

1.1 Propósito

Este documento es el plan de recuperación de desastres para la Universidad de Puerto Rico en Humacao del departamento de Sistemas de Información Computación y Comunicación. La información contenida es una guía en la que se establecen las normas y los procedimientos que se utilizarán en caso de emergencia. El empleo de éstas capacitarán a la administración Universitaria y el personal técnico del SICC a responder asertivamente en caso de ocurrir un evento que destruya todas o parte de la las facilidades del centro de cómputos de la UPR en Humacao. Además para reducir el impacto negativo de eventos que puedan afectar a los Sistemas de Información, Computación y Comunicación de la UPRH. .

1.2 Alcance

En la actualidad el Centro de Cómputos ofrece servicios de computación, tanto al área administrativa como a la académica. Es importante señalar que parte de un Plan de Recuperación de Desastres es identificar aquellas áreas que tienen prioridad y que por su naturaleza pueden afectar el funcionamiento administrativo de la institución si no se cuenta con el servicio que las mismas ofrecen. Este plan identifica como prioridad el área administrativa y todos los sistemas que operan bajo ésta, actualmente. (Ver apéndice A). El lugar designado es en la OSI de la Oficina del Presidente de la UPR.

2 Recursos de Computación

Actualmente el Centro de Cómputos cuenta con los siguientes computadores, catalogados como "Mainframes".

2.1 Mainframe
- 2.1.1 Digital Alpha, modelo DS20e (Computador Administrativo)
- 2.1.2 2GB de memoria
- 2.1.3 13 discos SCSI
- 2.1.4 1 procesador de 833 Mhz
- 2.1.5 Unidad de Cinta DLT 8000 (En la OSI-AC es una TZ88)

2.2 Servidores
- 2.2.1 Webmail
- 2.2.2 DHCP (dos - uno por segmento)
- 2.2.3 Intranet
- 2.2.4 Track-It
- 2.2.5 Web Server
- 2.2.6 SQL Server

3 Personal

A continuación se menciona el personal del Centro de Cómputos que componen el Comité de Desastre que estará a cargo de activar este Plan de Recuperación de Desastres. Además, se menciona aquel personal externo del cual se requiere su colaboración.

3.1 Personal a cargo de activar el plan.

3.1.1 Director(a) de Oficina Sistemas de Información, Computación y Comunicación (SICC)

Milagros Morales
Tel. Ofi. (787) 850-9307
Tel. Res. (787) 733-0579
Tel. Cel. (787) 214-1078

3.1.2 Director(a) de División de Desarrollo Tecnológico

Víctor D. Santiago
Tel. Ofi. (787) 850-9382
Tel. Res. (787) 733-3282

3.1.3 Director(a) de Operaciones y Procesamiento de Datos

Héctor R. López/Luis O. Rojas
Tel. Ofi. (787) 850-9366
Tel. Celular; (787) 568-2282 (Héctor R. López)
Tel. Celular; (787) 615-7556 (Luis O. Rojas)

3.1.4 Especialista de Telecomunicaciones

Cándido Flecha
Tel. Ofi. (787) 850-9312
Tel. Res. (787) 285-2887

3.1.5 Especialista de Sistemas Operativos (encargado del computador Alpha)

Ernesto Soto
Tel. Ofi. (787) 850-9312
Tel. Res. (787) 839-5150
Tel. Cel. (787) 501-0583

3.2 Personal externo del cual se requiere colaboración. (Ver Apéndice C)

3.2.1 Oficina del Presidente

3.2.1.1 Coordinador de OSI-AC
Julia Celeste Bartolomei
Tel. Oficina (787)250-0000 ext 3101
Tel. Celular (787) 616-2399

3.2.1.2 Director de Operaciones OSI-AC
Amed Medina
Tel. Oficina (787) 250-0000 ext 5401

3.2.2 International Safe Deposit
Tel. (787) 792-9877

3.2.3 Oficiales de la UPRH

3.2.3.1 Directora de Nómina
Marta Santiago
Tel. Oficina (787) 850-9358
Tel. Residencia (787) 850-0756
Tel. Celular (787) 637-0504

3.2.3.2 Directora de Recursos Humanos
Eduardo Clemente
Tel. Oficina (787) 850-9358
Tel. Residencia (787)
Tel. Celular (787)

3.2.3.3 Directora de Recaudaciones
Wanda G. Díaz
Tel. Oficina (787) 850-9358
Tel. Residencia (787) 850-3198
Tel. Celular (787) 384-7121

3.2.3.4 Registrador
Jorge L. Acevedo
Tel. Oficina (787) 850-9358
Tel. Residencia
Tel. Celular (787) 309-9225

3.2.3.5 Directora de Finanzas
Inés Sánchez Mercado
Tel. Oficina (787) 850-9358
Tel. Residencia (787) 266-5963
Tel. Celular (787) 903-0384

3.2.3.6 Director de Contabilidad
Lydia Casas
Tel. Oficina (787) 850-9358
Tel. Residencia (787) 736-1230
Tel. Celular (787) 385-1230

3.2.3.7 Directora Cuentas por Pagar
Luz E. Rosario
Tel. Oficina (787) 850-9358
Tel. Residencia (787) 852-0229

3.2.3.8 Directora de Asistencia Económica
Mariolga Rotger
Tel. Oficina (787) 850-9358
Tel. Residencia (787) 874-6476
Tel. Celular (787) 370-4184

3.2.3.9 Director Oficina Fiscal de Asistencia Económica
Alfredo Aponte
Tel. Oficina (787) 850-9358
Tel. Residencia (787) 285-2643
Tel. Celular

3.2.3.10 Coordinador de Recursos Físicos
Ing David Laboy
Tel. Oficina (787) 850-9358
Tel. Residencia: 475-7376

4 Plan de Acción

El Director del SICC-UPRH o persona designada por éste declarará la emergencia y contactará al Rector/a de la institución y a su vez al Director de OSI-AC o persona designada por ésta para activar el Plan de Recuperación de Desastres. Este plan se activará en conjunto con el de la institución. (Ver Anejo F)

5 Situaciones Cubiertas y Objetivos

A continuación se enumerarán las situaciones o eventos que pueden afectar la operación del SICC y la acción a tomar durante el mismo. Se considerarán eventos críticos entre otros.

5.1 Falla en el funcionamiento del computador Alpha DS20e

Hay que tomar especial atención a las siguientes aplicaciones que componen los sistemas administrativos:

5.1.1 Sistema Financiero (FRS)
5.1.2 Sistema Estudiantil (SIS)
5.1.3 Sistema de Recursos Humanos (HRS)

En caso de que éste falle y se prolongue, el personal encargado de los sistemas críticos se reunirán para determinar si es necesario utilizar las instalaciones de la Oficina de Sistemas de Información en la Oficina del Presidente (OSI-AC).

5.2 Interrupción prolongada de electricidad

5.2.1 Definición - La falta de energía eléctrica en todo el Colegio por un periodo mayor de 24 horas.

5.2.2 Objetivos

5.2.2.1 Suplir energía eléctrica al SICC mediante sus sistemas de emergencia (UPS y generador).

5.2.2.2 En sus instalaciones, se habilitarán espacios de trabajo temporeros para realizar las funciones esenciales.

5.2.3 Falla en el funcionamiento de uno de los discos magnéticos donde se almacenan las aplicaciones y datos de producción.

De surgir algún problema con algún disco que se afecten alguna aplicación o datos se tomará la acción de:

5.2.3.1 Se identifica el disco disponible para estos casos.

5.2.3.2 Se restaura con el resguardo más reciente.

5.2.3.3 Las tres aplicaciones críticas (FRS, SIS, HRS) poseen un sistema de reguardo de transacciones en línea. Éste nos permite restaurar hasta la última transacción afectada antes de ocurrir un daño al disco magnético. Se aplica el *Check Pointer* a la aplicación correspondiente.

5.2.3.4 Una vez restaurado el disco se renombra el directorio afectado.

5.2.3.5 El Área de Operaciones es la responsable de efectuar la restauración de las aplicaciones y datos.

5.3 Desastre limitado al SICC

5.3.1 Definición - Un desastre que impida la operación del SICC por más de 48 horas, pero que no afecte el funcionamiento del resto de la UPRH.

5.3.2 Objetivos

5.3.2.1 Se realizarán todas las funciones administrativas y académicas de la UPRH y se efectuarán los trabajos computadorizados necesario en un lugar alterno durante la noche..

5.3.2.2 En esta situación, se emitirán los cheques de nómina de empleados, de estudio y trabajo y de becas, de acuerdo con sus respectivos calendarios

5.3.2.3 Se restablecerán los servicios administrativos computadorizados, en la misma localización o en una diferente dentro de un plazo de no más de 30 días.

5.3.2.4 Se entregarán, a petición de sus dueños, los datos almacenados en el sistema administrativo que se necesiten con urgencia. El Comité de Desastre decidirá la prioridad de las peticiones.

5.3.3 **Inundación**

5.3.3.1 Inundación dentro de un espacio reducido del Centro de Cómputos

5.3.3.1.1 El Director del SICC o persona designada por éste se comunicará con la Oficina de Recursos Físicos de la UPRH para establecer el plan de limpieza del área afectada.

5.3.3.1.2 Se reanudarán las operaciones tan pronto se realice la limpieza.

El SICC cuenta con un sistema de sensores que detectan la humedad en el Cuarto de Máquinas.

5.3.3.2 Inundación en la totalidad del SICC

5.3.3.2.1 Se apagarán y desconectarán todos los equipos de no haber riesgos; si existe algún riesgos se desconectará la corriente por el interruptor principal.

5.3.3.2.2 El personal del SICC se reubicará dentro de las áreas disponibles las cuales se puedan designar para establecer las operaciones de éste.

5.3.3.2.3 El Director del SICC o persona encargada se comunicará con la Oficina de Recursos Físicos para establecer el plan de limpieza del área afectada.

5.3.3.2.4 Se evaluará la necesidad de adquirir nuevo equipo o se evaluará la garantía, seguros, etc.

5.3.3.2.5 Si la situación se prolongara por más de un día, habrá que ponerse en contacto con las personas claves de las aplicaciones críticas para identificar la necesidad de mover su personal a las instalaciones de la OSI-AC.

5.3.3.2.6 Una vez se normaliza la situación, se realiza un resguardo de los datos procesados en esa instalación y se restaurará el mismo en el SICC para proseguir el funcionamiento normal de los sistemas.

5.3.4 **Amenaza de Bomba**

5.3.4.1 Seguiremos el plan de respuesta de emergencias institucional de la UPR Humacao establecido en la pag. 25

5.3.5 **Tormentas y Huracanes**

5.3.5.1 Seguiremos el plan de respuesta de emergencias institucional de la UPR Humacao establecido en la pag. 10

5.3.6 **Terremotos**

5.3.6.1 Seguiremos el plan de respuesta de emergencias institucional de la UPR Humacao establecido en la pag. 29

5.3.7 Fuego

El SICC cuenta con detectores de humo, que al momento de detectar una situación de fuego, se activará en forma automática (ver Apéndice ___. Este sistema rocía el área donde se encuentra el equipo con una sustancia que evita el daño de los equipos.

5.3.7.1 El Director del SICC o persona designada por éste se comunicará con el comité de emergencias de la UPR en Humacao para que active el plan de respuesta y coordine el plan de limpieza del área afectada.

5.3.7.2 El personal designado en el SICC evaluará la extensión de los daños al equipo; la necesidad de adquirir nuevo equipo o se evaluará la garantía, seguros, etc.

5.3.7.3 Si la situación se prolongara por más de un día, habrá que ponerse en contacto con las personas claves de las aplicaciones críticas para identificar la necesidad de mover su personal a las instalaciones de la OSI-AC.

5.3.7.4 Se continuará operando desde las instalaciones de la OSI-AC hasta que se normalice la situación y el computador vuelva a estar en funcionamiento.

5.3.7.5 Una vez se normalice la situación se realizará un resguardo de los datos procesados en esa instalación y se restaurará en el SICC para proseguir el funcionamiento normal de los sistemas.

5.4 Huelga en la UPRH

Una vez comienzan los rumores de que se iniciará un periodo extenso de huelga:

5.4.1 Se procederá a realizar un resguardo general de todos los sistemas administrativos.

5.4.2 Se llevará el resguardo a la Compañía International Safe Deposit diariamente.

5.4.3 Las oficinas responsables de los sistemas críticos determinan el material y la cantidad del mismo que necesitan y pasan por el SICC para recoger este material.

5.4.4 El día que da comienzo la huelga, el personal designado por cada sistema crítico se traslada al local que se ha seleccionado para continuar realizando las operaciones de los sistemas.

5.4.5 Una vez se normaliza la situación, se realiza un resguardo de los datos procesados en esa instalación y se restaura el mismo en el SICC para proseguir el funcionamiento normal de los sistemas

5.5 Falla de electricidad en el SICC

Actualmente los equipos están conectados al UPS y éste a su vez está conectado al generador de electricidad para el SICC. El UPS nos permite hasta 15 minutos de funcionamiento en lo que se activa el generador. De haber problemas con la activación del generador se hará lo siguiente:

5.5.1 El Director del SICC o persona encargada solicitará información a la Oficina de Recursos Físicos de la UPRH sobre la falla.

5.5.2 Se evaluará la situación y de ésta prolongarse se tomará la decisión de moverse o no a la OSI-AC luego de haberse reunido con los custodios de los sistemas críticos.

5.6 Falla de electricidad en la UPRH

5.6.1 El Director del SICC o persona designada solicitará información a la Oficina de Recursos Físicos de la UPRH sobre la falla.

5.6.2 Se evaluará la situación y de ésta prolongarse por mas de un día y estar sin el servicio del generador eléctrico, se pondrá en contacto con los custodios de los sistemas críticos para identificar la necesidad de mover su personal a las instalaciones de la OSI-AC.

5.7 Desastre total

5.7.1 Definición Un desastre se refiere cuando se hace inoperante a la mayor parte de la UPRH.

5.7.2 Objetivos

5.7.2.1 Emitir en el lugar alterno los cheques de nóminas de empleados, de estudio y trabajo y de becas, de acuerdo con sus respectivos calendarios.

5.7.2.2 Restablecer los servicios académicos y administrativos lo antes posible.

5.7.2.3 El Comité de Desastre decidirá la prioridad de las peticiones.

5.8 El Comité de Desastre del SICC (ver página 5) determinará los pasos específicos a efectuarse para lograr las metas

5.8.1 Fecha en que comenzará la labor en el lugar alterno.

5.8.2 Personas que irán a trabajar cada tarde al lugar alterno.

5.8.3 Cómo se rehabilitará el SICC.

5.8.4 En esta situación se emitirán los cheques de nómina de empleados, de estudio y trabajo y de becas de acuerdo con sus respectivos calendarios.

5.8.5 Se realizarán todas las funciones administrativas y académicas de la UPRH y se efectuarán los trabajos computadorizados necesarios en el lugar alterno durante la noche.

5.8.6 Se restablecerán los servicios académicos y administrativos computadorizados en la misma localización o en una diferente dentro de un plazo de no más de 30 días.

5.8.7 El Comité de Desastre decidirá la prioridad de las peticiones.

6 Cadena de Mando y Declaración de Desastre

Las siguientes personas componen la cadena de mando para enfrentar una de las situaciones de desastre descritas. Ver el anejo F pag. 4 a 7 para conocer las responsabilidades de cada miembro.

6.1 Personas que componen la cadena de mando

6.1.1 Rectora de la UPRH

Nombre : Dra. Hilda M. Colón Plumey
Tel. Ofi. : (787) 850-9375
Tel. Res : (787) 743-0857
Tel. Cel. : (787) 307-1107
Oficina : Edificio de Administración
Residencia : Urb Altos de la Fuente C2 E5
Caguas PR

6.1.2 Decanato Académico

Nombre : Dr. José M. Encarnación
Tel. Ofic. : (787) 850-9303
Tel. Res : (787) 889-6036
Tel. Cel. : (787) 920-0607
Oficina : Edificio de Administración
Residencia :

6.1.3 Decanato Estudiantil

Nombre : Dr.Carlos Rubén Carrasquillo
Tel. Ofic. : (787) 850-9328
Tel. Res : (787) 746-4874
Tel. Cel. : (787) 920-0608, 685-2790
Oficina : Edificio de Servicios al Estudiante (Antigua Biblioteca)
Residencia :

6.1.4 Decanato Administrativo

Nombre : Sra. Daisy Rivera
Tel. Ofic. : (787) 850-9324
Tel. Res : (787) 733-5484
Tel. Cel. : (787) 920-0609
Oficina : Edificio de Administración
Residencia : Urb. April Garden
Las Piedras PR

6.1.5 Director del SICC

Nombre : Sra. Milagros Morales
Tel. Ofic. : (787) 850-9312
Tel. Res : (787) 733-0579
Tel. Cel. : (787)2 14-1078
Oficina : Edificio Ciencias Naturales
Residencia : Bo. Tejas
Las Piedras PR

6.1.6 Director de Análisis y Programación

Nombre : Sr. Víctor D. Santiago Álvarez
Tel. Ofic. : (787) 850-9312
Tel. Res : (787) 733-3282
Oficina : Edificio Ciencias Naturales
Residencia : Bo Tejas Villas del Río
Humacao PR

6.1.7 Especialista en Sistemas Operativos

Nombre : Sr. Ernesto Soto
Tel. Ofic. : (787) 850-9312
Tel. Res : (787) 839-5150
Tel. Cel. : (787) 501-0583
Oficina : Edificio Ciencias Naturales
Residencia : Bo Recio Calle Buena Vista
Patillas PR

6.1.8 Supervisor de Operaciones

Nombre : Sr. Héctor López
Tel. Ofic. : (787) 850-9366
Tel. Res : (787) 852-1817
Tel. Cel. : (787) 568-2282
Oficina : Edificio Ciencias Naturales

6.1.9 Coordinador de Emergencias de la UPRH

Nombre	: Oscar E. Rodríguez
Tel. Ofic.	: (787) 850-9377
Tel. Res	: (787) 285-0159
Tel. Cel.	: (787) 617-0619
Oficina	: Edificio de Administración
Residencia	: Urb Villa Universitaria Humacao PR

6.1.10 Coordinador de Emergencias de la UPRH Alterno

Nombre	: Sr. Carlos Figueroa
Tel. Ofic.	: (787) 850-9377
Tel. Res	: (787) 285-0159
Tel. Cel.	: (787) 617-0619
Oficina	: Edificio de Administración
Residencia	: 920-0613, 643-9212

6.2 Procedimiento

En una situación de emergencia la persona de mayor jerarquía en la cadena de mando que esté presente o en comunicación por teléfono o radio:

6.2.1 Asumirá el mando y la responsabilidad;

6.2.2 Iniciará las acciones necesarias de acuerdo con el Plan;

6.2.3 Se comunicará con una persona de mayor jerarquía en la cadena de mando;

6.2.4 Convocará a una reunión al Comité de Desastre.

6.3 El Coordinador de Contingencias

El(la) Rector(a) de la UPRH designará un Coordinador de Contingencias para mantener el Plan actualizado y concertar la relación con el Coordinador de Emergencia de la UPRH.

7 Itinerarios de Trabajos por Sistemas y Aplicaciones

En caso de emergencia se trabajará con las prioridades del Área de Operaciones de acuerdo con las necesidades del mismo. Por ejemplo, se dará prioridad a las nóminas y a los ciclos diarios, ya que en estos se producen los cheques de cuentas a pagar.

Trabajos que se realizan en el Centro de Cómputos (Área de Operaciones)

7.1 Ciclos Diarios

- 7.1.1 Ciclo Diario de Compras
- 7.1.2 Ciclo Diario de A/P (Cuentas a Pagar)
- 7.1.3 Ciclo Diario de Cheques
- 7.1.4 Ciclo Diario de F/A (Cuentas Financieras)
- 7.1.5 Ciclo Diario de Recaudaciones

7.2 Ciclos semana

- 7.2.1 Ciclo Semanal de Compras
- 7.2.2 Ciclo Semanal F/A

Nota: estos ciclos se procesan todos los viernes.

7.3 Ciclos Mensuales

- 7.3.1 Ciclo Mensual de Compras
- 7.3.2 Ciclo Mensual A/P
- 7.3.3 Ciclo Mensual F/A

Nota: estos ciclos se procesan el último día laborable del mes.

7.4 Ciclos Anuales

- 7.4.1 Ciclo Anual de A/P
- 7.4.2 Ciclo Anual de Compras
- 7.4.3 Ciclo Anual de F/A

Nota: estos ciclos se procesan en el Cierre de Año Fiscal.

7.5 Nóminas

7.5.1 Nómina Regular de empleados (1ra y 2da quincena)
7.5.2 Libros, descuento de matrícula y tres pagos de beca (se efectúa semestralmente)
7.5.3 Estudio y Trabajo (1 al mes)
7.5.4 Bono de Navidad
7.5.5 Banco de Licencia
7.5.6 Obvención

8 Peticiones de Usuarios

8.1 Peticiones de los usuarios de los Sistemas de FRS, HRS y SIS

8.1.1 Reconciliaciones Bancarias

8.1.2 Procesos que se corren de los archivos del Banco 29, Banco 26 y Banco 21

8.1.3 Transferencias de Archivos al Banco

8.1.4 Proceso de bajar los archivos del Banco para poder realizar las reconciliaciones bancarias

8.1.5 Corrección de Exámenes

8.1.6 Lectura de Listas de Clases

Procesar listas de clases y notas de la Oficina del Registrador.

9 Sistemas o Aplicaciones con las que se utilizan en el Centro de Cómputos

9.1 Aplicaciones críticas

9.1.1 FRS - se utiliza para correr todos los procesos del Sistema Financiero.
9.1.2 SIS - se utiliza para correr todos los procesos del Sistema Estudiantil.
9.1.3 HRS - se utiliza para correr todos los procesos del Sistema Recursos Humanos.

10 Inventario de Equipo y Materiales a Utilizar en una Emergencia

En caso de emergencia se necesita todo el equipo y algunos materiales de los antes descritos para poder generar los trabajos de mayor prioridad que se realizan en el Centro de Cómputos. Según acuerdos anteriores el equipo nos lo puede proveer la Oficina de Sistemas de Información de Administración Central. En cuanto a materiales la Oficina de Pagaduría nos debe proveer los cheques. Dependeríamos de la Administración Central para que nos faciliten papel para imprimir los informes que sean más necesarios.

10.1 Equipo

10.1.1 DLT TAPE IV (unidad de resguardo)
10.1.2 Discos duro de Alpha
10.1.3 Terminales de trabajo
10.1.4 Impresora LG06, LP27
10.1.5 Laser HP 8150
10.1.6 Scantron 8200
10.1.7 Alpha Server DS20e

10.2 Materiales

10.2.1 Cheques del banco 29 (cuentas a pagar)
10.2.2 Cheques del banco 26 regular (nóminas)
10.2.3 Talonario 26 depósito directo (nominas)
10.2.4 Cheques del banco 21 (beca y estudio y trabajo)
10.2.5 Papel normal 14 7/8 x 8 ½
10.2.6 Papel de 4 partes 14 7/8 x 11
10.2.7 Papel 8 x 11 perforado
10.2.8 DLTTAPE IV (para realizar resguardo) actualmente tenemos seis disponibles para emergencias en International Safe Deposit Corp.
10.2.9 Diskettes 3.5

10.3 Archivos y Programas

Estos se encuentran en "backups". Los "backups" diarios y semanales se guardan en la bóveda del SICC y los "backups" mensuales y anuales se guardan en la compañía externa International Safe Deposit Corp.

11 Procedimiento para la Normalización de las Operaciones después del Desastre

Realizar un resguardo de todos los procesos que se ejecuten durante la emergencia para poder actualizar nuestros archivos y restaurar los datos en la unidad permanente de trabajo.

12 Planes de Contingencias

12.1 Desastre Tipo A - Interrupción Prolongada de Electricidad

12.1.1 Se suplirá energía eléctrica al SICC mediante sus sistemas de emergencia (UPS y generador).

12.1.2 El Comité de Desastre se reunirá y determinará las tareas esenciales que se realizarán a pesar de la ausencia de electricidad en el resto de la UPRH.

12.1.3 Se habilitará espacios de trabajo temporeros para realizar estas funciones en el SICC.

12.2 Desastre Tipo B - Desastre Limitado al SICC

12.2.1 El Coordinador de Contingencia convoca al Comité de Desastre. El Comité quedará constituido con la presencia de dos o más de las personas que lo componen.

12.2.2 El Comité determinará los pasos específicos a efectuarse para lograr las metas trazadas en este plan:

12.2.2.1 Se habrá de establecerse un lugar de procesamiento alterno en la UPRH. Esto podrá hacerse bajo ciertas circunstancias a través de la adquisición de equipo nuevo o la reparación del equipo existente y su instalación en un lugar de la UPRH que no se haya afectado por el desastre, que tenga corriente eléctrica y acondicionador de aire y que no esté muy distante de la red UPRHNet;

12.2.2.2 La fecha en que comenzará la labor en el lugar alterno;

12.2.2.3 Las personas que irán a trabajar cada tarde al lugar alterno;

12.2.2.4 Cómo se rehabilitará el SICC.

12.3 Desastre Tipo C – Desastre Total

Se emitirán en el lugar alterno los cheques de nóminas de empleados, de estudio y trabajo y de becas, de acuerdo con sus respectivo calendarios. Los servicios académicos y administrativos se re-establecerán tan pronto como sea posible.

12.3.1 El Coordinador de Contingencias convocará al Comité de Desastre. El comité quedará constituido con la presencia de dos o más de las personas que lo componen.

12.3.2 El comité determinará los pasos específicos a efectuarse para lograr las metas trazadas en este plan:

12.3.2.1 La fecha en que habrá de comenzar la labor en un lugar alterno;

12.3.2.2 Las personas que irán a trabajar cada tarde al lugar alterno;

12.3.2.3 Cómo se rehabilitará el espacio del Centro de Cómputos en armonía con los planes de rehabilitación para el Colegio en su totalidad.

13 Programa de Preparación para Contingencias

La UPRH llevará a cabo un programa sistemático de adiestramiento para, en caso de desastre, garantizar que el Colegio esté preparado. El Coordinador de Contingencias de la UPRH será el responsable de la ejecución de este programa.

El supervisor del área de operaciones del Centro de Cómputos será responsable de ejecutar este Programa. El programa de resguardo definido en el documento *Normas y Procedimientos sobre el Uso de Recursos de Computación.*

13.1 **El programa de mantenimiento del sistema de control de fuego en el Centro de Cómputos**. El Director del Centro de Cómputos será responsable de que el personal experto en el área realice, por lo menos, dos inspecciones anuales al sistema para que se mantenga en óptimas condiciones. Además, se llevará un registro de las inspecciones y de las reparaciones efectuadas.

13.2 **El programa de mantenimiento del suministro alterno de electricidad.** El Director de la División de Recursos Físicos de la UPRH serán responsable de establecer y mantener:

13.2.1 un programa de pruebas semanales del generador de electricidad;
13.2.2 un registro de las pruebas efectuadas con resultados y observaciones;
13.2.3 un programa de mantenimiento del equipo y de las instalaciones eléctricas;
13.2.4 un sistema de inspecciones que garantice un suministro de combustible para una operación continua de 30 días.

13.3 **Un acuerdo con un lugar alterno para laborar**. El Director del SICC mantendrá un acuerdo para laborar en un lugar alterno. Así se garantizará el cumplimiento de las metas de este Plan de Recuperación de Desastress. El Director del SICC será responsable de establecer y mantener vigente este acuerdo. Para que no se ocasionen gastos, se espera que este contrato se haga con otro Recinto de la UPR y que la relación sea una de naturaleza mutua. Esto implica que NO SE CONTEMPLA MANTENER NINGÚN SERVICIO si la Universidad de Puerto Rico está inoperante.

13.4 **El programa de cheques de emergencia.** El Director de Finanzas de la UPRH será responsable de almacenar en el sitio alterno una cantidad de cheques que sea suficiente para los pagos de 30 días.

13.5 **El programa de simulacros anunciados**. Una vez al año se efectuará un simulacro anunciado para poner en práctica el plan en el lugar alterno. Se recogerá el último resguardo de la compañía International Safe Deposit; se llevará al sitio alterno; personal de finanzas, contabilidad, asistencia económica y nóminas hará transacciones en el lugar

alterno; y se producirá una nómina hasta la impresión de cheques en papel corriente. Estas actividades se llevarán a cabo en el horario determinado en el acuerdo entre la UPRH y el lugar alterno. Los directores de cada una de las oficinas mencionadas serán responsables de lograr que un representante idóneo participe en el simulacro.

13.6 **El programa de simulacros no anunciados**. Una vez al año se efectuará un simulacro de desastre que se anuncia por la mañana del día en que se va a efectuar. Los Coordinadores de Contingencias y de Emergencias de la UPRH serán responsables de determinará al fecha de los simulacros (anunciado y no anunciado); velar por su ejecución y que se tomen medidas correctivas para los problemas que se detecten en ellos. Los directores de cada una de las oficinas antes mencionadas serán responsables de lograr que un representante idóneo participe en le simulacro. Estas actividades también se levarán a cabo en el horario determinado en el acuerdo entre la UPRH y el lugar alterno.

13.7 El(la) Coordinador(a) de Contingencias de la UPRH radicará un informe a la Junta Administrativa sobre los resultados de cada simulacro no más tarde 30 días después de efectuados los mismos.

14 Revisión del Plan

Este documento debe ser revisado anualmente por el Director(a) de SICC o persona designada por la autoridad nominadora del UPRH y discutido junto a todo el personal envuelto en el plan de acción.

Dra. Hilda M. Colón Plumey
Rectora

Fecha

Sr. Ernesto Soto
Director SICC

Fecha

C:\www_uprh_edu\oficinas\sicc\Plan-Contingencias.wpd

Apéndices

Apéndice A
Registro de Prueba del Plan de Recuperación de Desastres

Fecha: **2-mar-2006** Personal Lugar Alterno: **Ahmed Medina. OSI Oficina del Presidente** Firma: _____

Hora Comienzo	Hora Terminado	Tareas Realizadas	Iniciales UPRH	Iniciales OSI
10:00AM		Simulación del Sistema de HRS		
		1 Entregamos la cinta de resguardo al Operador, Sr. John De Micheli, para comenzar a restaurar la información.		
		2 Hubo problemas con la lectura de la cinta. La densidad de la unidad de cinta (DLT 8000) a la que se guardaron los datos en la UPRH no era compatible con la unidad de la OSI-AC (TZ88).		
		3 Se procedió con la creación de los directorios necesarios para restaurar los datos en OSI-AC.		
		4 Debido al problema mencionado en el ítem 2, se bajaron los datos por la red para probar los directorios creados y dejar establecido toda la estructura requerida.		
	3:00PM	5 Se probó la entrada a HRS: (1) se corrió un borrador de nómina; (2) se hicieron cambios en línea y se corrió nuevamente el borrador de nómina; (3) se verificó que los cambios estuvieran reflejados en la nómina. Los resultados fueron exitosos.		
		6. En OSI-UPRH se procedió a hacer un resguardo con la densidad que fuera compatible con la unidad de cinta de la OSI-AC para ir antes de la fecha de la prueba real del Plan de Recuperación de Desastres.		
		7. Se estableció que el martes 7 de marzo de 2006 se realizará la prueba real para HRS.		

Fecha: **7-mar-2006** Personal Lugar Alterno: **Ahmed Medina**, OSI Oficina del Presidente Firma: _____

Hora Comienzo	Hora Terminado		Tareas Realizadas	Iniciales UPRH	Iniciales OSI
			Simulación del Sistema de HRS		
10:20AM	4:40PM	1	Bajar los datos de la cinta de Humacao en OSI-AC. Hubo problemas al bajar los datos: (a) problemas con las versiones ; (b) cinta magnética de OSI-AC muy lenta.		
4:41PM	4:45PM	2	Se creó un borrador de la primera quincena de marzo para compararlo con el que se trajo de Humacao. EJCALC.COM. Salió bien		
4:46PM	**4:50PM**	3	**Se hizo un cambio real en línea.**		
4:52PM	4:54PM	4	Se corrió nuevamente un borrador y verificó que todo saliera con los cambios.		
4:57PM	5:00PM	5	Se corrió un EJBACKUP.		
5:07PM	5:18PM	6.	**Se corrió el EJCALC_FINAL**		
5:19PM	**5:28PM**	7.	**Se corrió EJCKR1 para actualizar los archivos históricos**		
5:29PM	**5:32PM**	8	EJBA**CKUP**		
		9	EJA520		
		10.	**EJLBR1**		
		11.	**EJU425_CUH**		
		12.	**EJC600**		
		13.	EJM578		
		14.	**EJBACKUP**		
		15.	**Impresión de talonarios e impresión de cheques**		
		16.	**Envío de depósito directo al BPPR**		
	8:00PM	17.	Backup en OSI-AC para restaurar en UPRH		
			(Ver Apéndice E - Solicitud de Proceso de Nómina Final)		

Apéndice B
Pre-Simulacro Nómina

I. Participantes

1.	Luis E. Soto	Director SICC
2.	Héctor Villalobos	Especialista en sistemas Operativos
3.	Víctor D. Santiago	Director de Análisis y Programación
4.	Angel L. Carrasquillo	Especialista en Tecnologías de Información
5	Héctor R López	Supervisor de Operaciones
6.	Marta Santiago	Directora de Nóminas
7	Marilú Dávila	Pagadora

II. Material necesario

1. Resguardo completo al 6-mar-06 de los siguientes discos:
   - a DKD300 - Sistemas
   - b. DKD1000 - Área datos de HRS
   - c. DKD400 - Área datos FRS
2. Cheques/Talonarios

III. Apagar el Check Pointer de HRS para que no actualicen los datos.

IV. Creación de cuenta HRS_PRODUCT_UPRH (uic: [773,2] [UPRH, HRS_PRD_UPRH])

V Creación de directorios

1. [CUHPRDZSS]
   [CUHPRDZSS.PRDZSSEXE]
   [CUHPRDZSS.PRDZSSDAT]
   [CUHPRDZSS.PRDZSSCOM]
2. [CUHPRDHRS]
   [CUHPRDHRS.PRDHRSEXE]
   [CUHPRDHRS.PRDHRSDAT]
   [CUHPRDHRS.PRDHRSCOM]
3. [PRDFRSDAT]
4. [PRDHRSDAT]
5. [PRDHRSPRT]

VI. Crear lógicos para los discos

1. DISK$PRDZSS
2. DISK$PRDHRS
3. DISK$PDSDAT
4. DISK$PDFDAT
5. DISK$PDHDAT
6. DISK$PRDFRS
7. DISK$PRDSIS
8. DISK$PRTHRS
9. DISK$PDZDAT

Ejemplo: $ define/system disk$pdsdat DKD900:

VII. Bajar backup en los directorios recien creados. EN el caso de FRS solo se necesita los archivos FOFILE, FSFILE, FGFILE, FBFILE.

VIII. Operador a utilizar, Marta Santiago

IX. Correr borrador EJCALC.COM y nómina final

X Revisar informes en pantallas

XI. Imprimir informes y cheques.

XII. Realizar un reguardo completo del disco utilizado para la simulada

XIII. Borrar directorios creados y usuario.

IVX. Restaurar en UPRH los directorios afectados (antes realizar un resguardo).

Notas:
1_ Disco utilizado - DKB6
2_ Editor que se utiliza en la OSI-AC es LSE
3. Luego de bajar los archivos, editar HR$COM:ZCTL03.com para comentar el cotejo de la hora.
4_ Editar el LOGIN.COM para cambiar el QUEUE IAS$BATCH por ACUPR1_SYS$BATCH en el símbolo SB de submit
5_ Verificar y ejecutar DKB6:[CUHPRDZSS]LOGICOS_UPRH.COM para asignar lógicos de discos
6. Las transacciones realizadas en línea de AC-OSI se guardan en el archivo ZAU003.DAT del sistema de OSI-AC con la letra W, no en el área nuestra HR$DATA:[PRDHRSDAT]ZAU003.DAT
7 QUEUE de impresión en OSI-AC ACUPR1_SYS$PRINT. Forma de cheques NOMHRS.
8 Extensión cuarto de Operaciones en OSI-AC 5428.

Apéndice C
Proceso para Restaurar Datos de HRS en OSI-AC

```
$!*************** RESTORE_PLAN_CONTIN_EN_AC.COM ***************
$!
$!    Proceso para restaurar backup de HRS en Alpha de OSI-AC
$!
$! Revisar nombre del          SAVE SET
$!
$ BACKUP/LOG/LIST=DKB6:[CUHPRDHRS]MAR0606FDKD3_HRS.LIS
$   MKC300:MAR0606FDKD3.SAV/SELECT=([CUHPRDHRS...]*.*;0)  -
$   DKB6:[CUHPRDHRS...]*.*/OWNER=PARENT
$ BACKUP/LOG/LIST=DKB6:[CUHPRDHRS]MAR0606FDKD3_ZSS.LIS -
   MKC300:MAR0606FDKD3.SAV/SELECT=([CUHPRDZSS...]*.*;0)
   DKB6:[CUHPRDZSS...]*.*/OWNER=PARENT
$ BACKUP/LOG/LIST=DKB6:[CUHPRDHRS]MAR0606FDKD4_FDAT.LIS
  MKC300:MAR0606FDKD4.SAV/SELECT=([PRDFRSDAT]FBFILE.DAT;0,
  FGFILE.DAT;0,FOFILE.DAT;0,FSFILE.DAT;0) -
  DKB6:[PRDFRSDAT]*.*/OWNER=PARENT
$ BACKUP/LOG/LIST=DKB6:[CUHPRDHRS]MAR0606FDKD10_HDAT.LIS
  MKC300:MAR0606FDKD10.SAV/SELECT=([PRDHRSDAT...]*.*;0)
  DKB6:[PRDHRSDAT...]*.*/OWNER=PARENT
$ exit
```

Apéndice D
Carta de los Resultados del Plan de Recuperación de Desastres del SICC a la Rectora

Apéndice E
Solicitud de Proceso de Nómina Final

Apéndice F
Plan de respuestas a Emergencias UPR Humacao

Agenda

- Dirección General de Operaciones de Banca Central (DGOBC)
- Incidentes
- Administración de la Continuidad de Negocio (ACN)
  - Ciclo de vida
- La ACN en Banxico
  - Normatividad
  - Responsabilidad de la DGOBC
  - Escenarios en la DGOBC
- Próximos pasos

> Todo plan de acción tiene costos y riesgos, pero estos son mucho menos que aquellos costos y riesgos que genera la inactividad
>
> John F. Kennedy

DGOBC

BANCO DE MEXICO

- Principales funciones
  - Instrumentar la Política Monetaria y la Política Cambiaria
  - Administración de las Reservas Internacionales
  - Agente financiero del Gobierno Federal

- Algunos números
  - Dos direcciones: Operaciones y Apoyo a las Operaciones
  - 45 aplicaciones: 20 críticas (< 1 día), 25 delicadas (< 1 semana).
  - 178 empleados (6% del total)
  - 45 en la GDSO
  - 3 encargados de la continuidad operativa

Incidentes

Predecibles

Inesperados

4/nov/2008 avionazo

Afortunados

Otros no tanto

Fuentes de incidentes

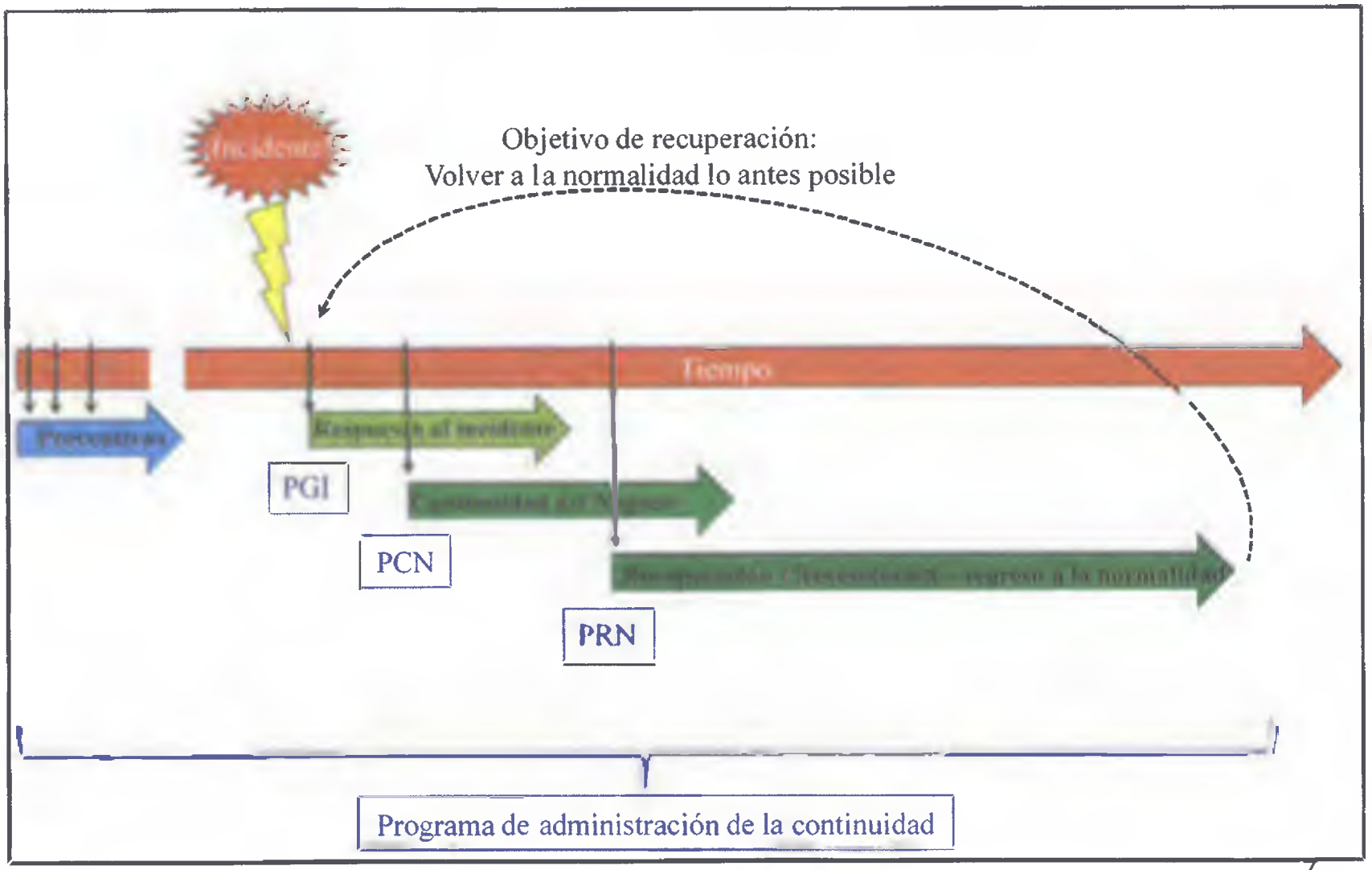
	Argentina	Brazil	Colombia	Costa Rica	Republica Dom.	Ecuador	El Salvador	Honduras	Mexico	Panama	Peru	Uruguay
Desastres Complejos	0	0	0	0	0	0	0	0	0	1	0	
Sequía	2	15	1	3	1	3	5	9	6	1	8	1
Actividad sísmica	5	2	23	13	2	16	10	6	27	4	39	0
Epidemia	2	15	2	1	5	11	9	7	3	5	11	0
Temperaturas Extremas	7	7	0	0	0	0	1	0	16	0	6	3
Inundación	46	104	61	23	17	24	14	25	55	27	38	12
Accidente Industrial	3	13	11	1	0	5	2	2	33	0	4	0
Infestación (Insectos)	0	1	1	0	0	0	0	0	0	0	1	0
Deslave (Seco)	0	0	1	0	0	1	0	1	0	0	2	0
Deslave (Mojado)	3	23	35	1	0	11	2	1	10	0	30	0
Accidentes Miscelaneos	6	22	10	2	2	4	3	5	14	6	10	0
Tormenta	17	18	7	8	25	0	11	19	75	4	3	0
Accidente de transporte	19	99	45	2	12	20	6	8	72	8	104	5
Actividad volcánica	2	0	11	6	0	10	1	0	10	0	2	0
Incendios Forestales	5	3	2	2	3	2	0	1	3	1	1	0

Fuente: Regional Business Forum BSI, Mario Ureña Cuate, 2011

Fuentes de incidentes para Banxico

- Capital - Distrito Federal
  - Zona metropolitana: 20kk, 2.5k hab/km^2
- Desastres naturales
  - Terremotos: 1957 (+7.3), 1985 (8.0 y 7.3)
  - Trombas: inundaciones (2m)
  - Pandemia: Influenza A (H1N1) abr/2009, 72k personas afectadas
- Situaciones humanas:
  - Acontecimientos políticos: 1994 (crisis del PRI), 2006 (plantón en Reforma)
  - Manifestaciones sociales: plantones, cierres, marchas (Centro Histórico)
  - Fiestas: 15/septiembre
  - Ataques de virus: ago/2003
  - Hundimiento de la ciudad: desbordamiento de ríos
  - Accidentes y errores

Atención de incidentes



Fuente: Norma BS 25999

Recursos críticos

- **Personal** – mantener las aptitudes y los conocimientos esenciales
- **Locales** – reducir el impacto de la indisponibilidad
- **Tecnología** – propia (procesos y sistemas) y de terceros (internos o externos)
- **Información** - asegurar la información vital
- **Suministros** – mantener la cadena de suministros
- **Grupos de interés** – proteger los intereses de los grupos de interés

Fuente: Norma BS 25999

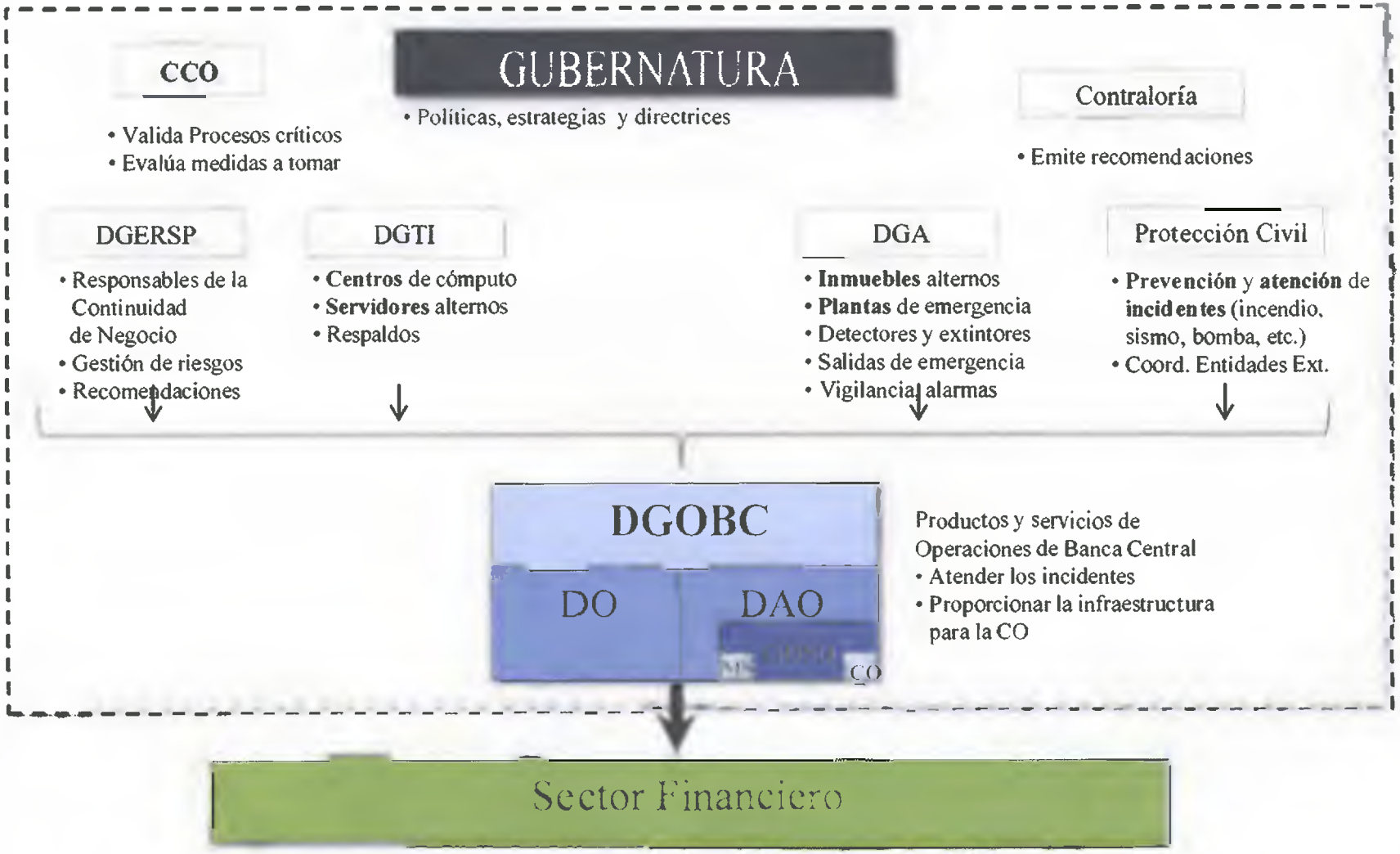
Administración de la continuidad del negocio (ACN)*

1. Administración del programa de ACN**
   - Facilitar el establecimiento y el mantenimiento de la capacidad de CN.
2. Entendimiento de la organización
   - Priorizar los productos y servicios, y los tiempos de entrega.
3. Determinación de la estrategia de ACN
   - Elegir las respuestas apropiadas para cada producto o servicio.
4. Desarrollo e implementación de la respuesta de ACN
   - Crear la infraestructura de atención de incidentes, continuidad de negocio y planes de recuperación.
5. Ejercicio, mantenimiento y revisión de la ACN
   - Permitir el ejercicio, mantenimiento, revisión y auditoría de la ACN.
6. Implantación de la ACN en la cultura de la organización
   - Permitir que la ACN se convierta en parte de los valores de la organización.

*Norma BS 25999 puedes y debes.

** En Banxico se utiliza el término Operativo en lugar de Negocio.

La ACN en Banxico



CO Grupo de Continuidad Operativa: una persona de tiempo completo y dos de tiempo parcial.
MS Mesa de Soporte: ocho personas- tres por día a tiempo completo.

Normatividad

La NAI Operación en Situaciones de Alerta

- Definiciones relevantes
- Las responsabilidades de los trabajadores y de la Unidades Administrativas
- Lo relativo a la declaración y conclusión de Alertas
  - El Gobernador es el encargado de efectuar la declaración de alerta Roja y de su conclusión.
  - El titular de la DGERSP es el encargado de efectuar la declaración de alerta Amarilla o Naranja, y de su conclusión
- La forma de proceder y de comunicarse en una Alerta
- Y lo que respecta a las situaciones no previstas.
- La DGERSP es la responsable de coordinar la continuidad operativa a nivel Institucional.

Semáforo de alerta

Una vez levantada una Alerta

Estados de alerta

		Alerta Amarilla	Alerta Naranja	Alerta Roja
Descripción del Estado de alerta		Se anticipa la ocurrencia de una **interrupción operativa mayor**	**Inminencia u ocurrencia de una interrupción operativa mayor**	**Ocurrencia de una interrupción operativa mayor**
Responsable de declarar y concluir el Estado de alerta		Director General de Sistemas de Pagos y Riesgos (Suplente: Director de Administración de Riesgos)		Gobernador (Suplente: Subgobernador que preside la Junta de Gobierno)
Nivel operativo de los procesos		Se ejecutan todos los procesos de forma cotidiana	Se ejecutan **todos los procesos** en la modalidad de continuidad operativa	Se ejecutan únicamente los **procesos críticos** y los de **apoyo a los críticos** en la modalidad de continuidad operativa
Roles de participación de los empleados	• Clave • Suplente	• **Ejecutar** todos sus procesos normalmente • **Informarse** sobre el rol de participación asignado para ejecutar los procesos en modalidad de Continuidad Operativa • **Repasar** los procedimientos que les aplican, relacionados con la operación en modalidad de Continuidad Operativa • **Estar atentos** a una posible declaración de Alerta Naranja o Alerta Roja.	• **Ejecutar** los Procesos en la modalidad de continuidad operativa conforme a las instrucciones establecidas por sus superiores. • **Estar atentos** a una posible declaración de Alerta Roja y adoptar las medidas preventivas adicionales que resulten pertinentes	• **Ejecutar** los Procesos Críticos bajo la modalidad de Continuidad Operativa y sus respectivos Procesos de Apoyo conforme a las instrucciones establecidas por sus superiores.
	• Apoyo		Deberán **permanecer en sus domicilios**, localizables y atentos a las instrucciones de sus superiores y/o a las que se difundan a través de los medios institucionales.	
Guías e instructivos de [illegible]			Instructivos, manuales o documentación elaborados para operar bajo la modalidad de continuidad operativa, emitidos por cada área.	
Información y contacto		Página de Alerta: www.banxico.org.mx/alerta Centro de Coordinación y Control (C3): 5268-8585		

Interrupción Operativa Mayor - retraso o interrupción significativo en Procesos Críticos o eventos que afecten la integridad de los trabajadores o de las instalaciones.

Continuidad Operativa – modalidad donde se ejecutan los procesos con el mínimo personal requerido.

Responsabilidad de la DGOBC

Por una vez

- Diseñar los documentos o instrucciones para operar en la modalidad de Continuidad Operativa y darlos a conocer.
  - MPO de Continuidad Operativa, PCO.
- Designar al Responsables de Continuidad Operativa y a su suplente y comunicarlo a la DAR.
  - El titular de la DO es responsable, el de la DAO, suplente.
- Designar al personal para ejecutar la modalidad de Continuidad Operativa.
  - Algunos escenarios tienen asignado personal específico.
- Determinar los roles de participación de sus trabajadores (clave, suplente, apoyo), y definir los medios o las vías para comunicarlos.
  - Está publicado en la página de continuidad de la DGOBC un catálogo con la clasificación del personal.

Responsabilidad de la DGOBC

Por evento

- Hacer de conocimiento de la DAR cualquier información que pudiera anticipar una interrupción operativa.
- El personal tiene que salvaguardar su integridad física, y consultar periódicamente la página de alerta hasta que se declare la conclusión de la alerta.

- Establecer el plan de acción particular ante la declaración de cada uno de los estados de alerta*

  La página Web de la DGOBC apunta a las instrucciones que se establecerán después de la evaluación de la situación (alcance e impacto) cuando suceda algún incidente.

  Tenemos y ejercitamos los escenarios que cubren los incidentes considerados de mayor impacto.

* Esta responsabilidad no forma parte de la Norma sin embargo se considera necesaria en caso de alguna contingencia.

Anexo 6

Continuidad Operativa en la Dirección General de Operaciones de Banca Central Banco de México

BANCO DE MEXICO

Continuidad Operativa en la DGOBC

Banco de México

BANCO DE MÉXICO

Septiembre, 2011

Obligaciones del Responsable de CO

- Servir de enlace con la DAR
- Contar en todo momento de un directorio del domicilio y teléfono de los trabajadores de los procesos críticos y los de apoyo, con las medidas de confidencialidad adecuadas
- Mantener actualizado el directorio
- Coordinar las labores para la elaboración y actualización de la documentación para la ejecución de los procesos en modalidad de Continuidad Operativa

Gestión de incidentes - PGI

Para la atención de incidentes existen tres niveles:

- Centro de Coordinación y Control (C3)
- El Centro de Soporte Institucional (CSI)
- La Mesa de Soporte

  Es la encargada de atender los incidentes relacionados con los sistemas de la DGOBC.

  Cuenta con prioridades, acuerdos de nivel de servicio y esquemas de escalamiento.

  Se apoya en el CSI para cuestiones de TI.

Escenarios y medidas implementadas*

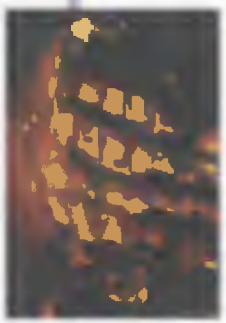
- Escenarios actualmente contemplados que pueden provocar una *posible interrupción de la operación de la DGOBC, y medidas preventivas* implementadas para mitigar su impacto:

Escenario	Medida
1. Imposibilidad de acceso o uso de las instalaciones primarias	Sitio de Operación Alterno
2. Contagio humano por virus epidemiológico (Alerta Sanitaria)	Operación Vía Remota
3. Falla de software en las ETB por contaminación por código malicioso, virus, gusanos, etc.	Red Protegida
4. Falla de servidores primarios	Servidores Alternos
5. Interrupción prolongada de la aplicación informática con que se opera	Planes de Continuidad de Negocio

*Estas medidas apoyarán la elaboración de los PCO de cada unidad administrativa.

1. Imp sibilidad de acceso uso de las instalaci nes primarias…

- Para cubrir este escenario, se cuenta con infraestructura alterna de trabajo, denominada Sitio de Operación Alterno (SOA).
- Proporciona los sistemas y servicios TI semejantes al sitio primario de trabajo (correo, extensiones telefónicas, faxes, impresoras, transporte, energía regulada, aire acondicionado, entre otros).
- Hay 79 módulos de trabajo designados para la DGOBC (44% del personal).
- Permite la operación en cualquier día hábil bancario.
- Para corroborar su funcionalidad, se opera en él diariamente.
- La información del contenido y como utilizar las instalaciones, se encuentra disponible en el Web interno del Banco.
- Se cuenta con un instructivo de bolsillo como apoyo al personal, para saber cómo actuar en caso de requerirse operar en el SOA.



1. Imp sibilidad de acceso uso de las instalaci nes primarias

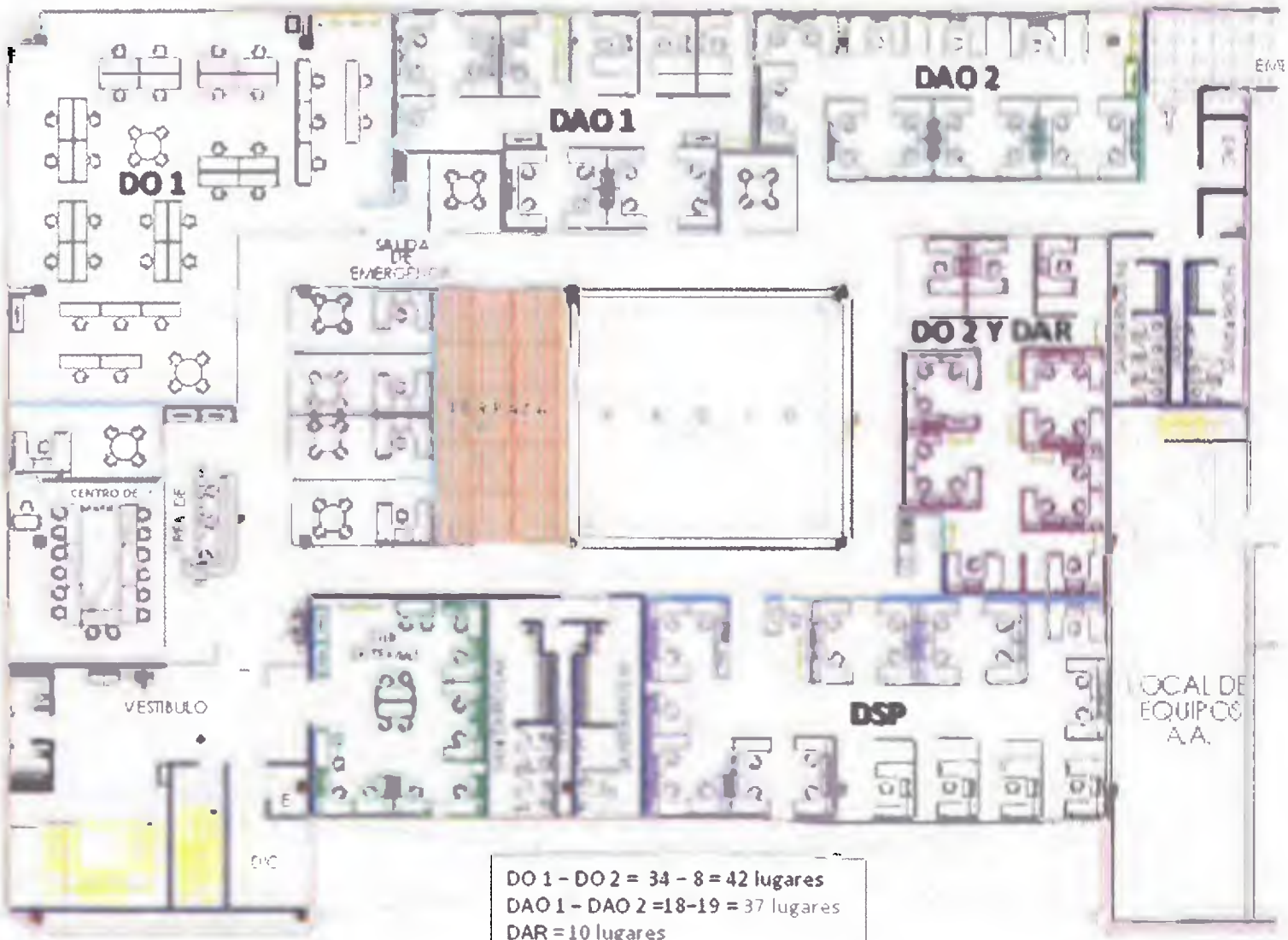
- Política de asistencia al SOA

DO - Personal de cada gerencia asiste una vez a la semana variando el día de la semana para ejecutar diferentes funciones.

DAO - Gerencia de Gestión de Operaciones - Asiste por lo menos una persona por oficina de lunes a viernes (promedio seis personas a la semana).

DAO - Gerencia de Desarrollo de Sistemas Operativos - Asisten en promedio seis personas cada lunes, miércoles y jueves, rolando su asistencia cada 15 días, procurando que siempre haya al menos un líder de especialidad en estos días.

SOA


DAO 1
DAO 2
DO 1
DO 2 Y DAR
DSP
VESTIBULO
LOCAL DE EQUIPOS A.A.
DO 1 – DO 2 = 34 – 8 = 42 lugares
DAO 1 – DAO 2 =18–19 = 37 lugares
DAR = 10 lugares
DSP = 27 lugares

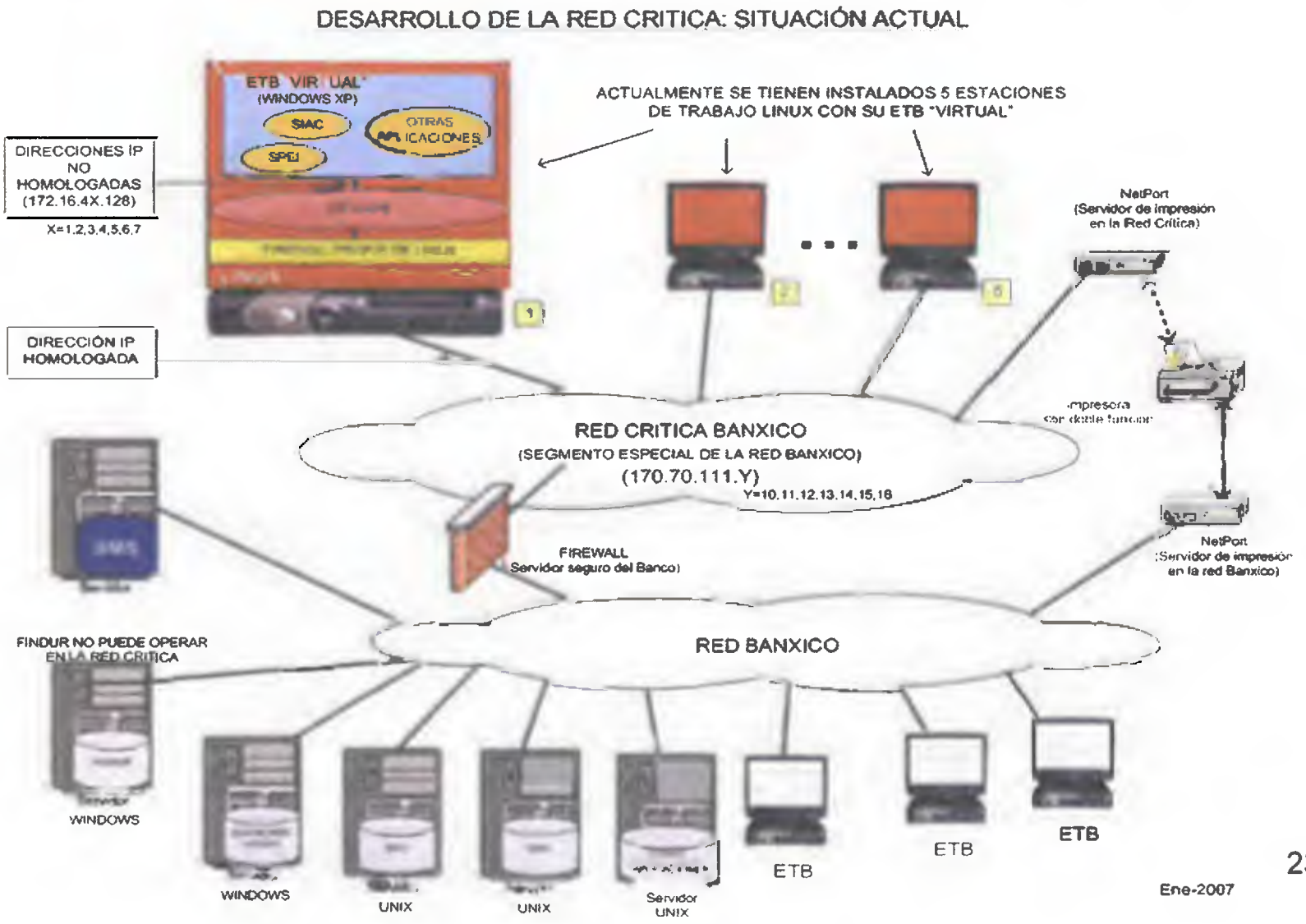
2. Contagio humano por virus epidemiológico

- Para cubrir este escenario, se proporcionó equipo de cómputo y telecomunicaciones a 25 personas de áreas operativas (14%), para que puedan conectarse vía Internet desde sus domicilios a sus equipos del Banco.
- Con esta medida se logra cubrir las funciones primordiales de la DGOBC en cualquier día hábil bancario.
- Este esquema fue utilizado en el año de 2009, durante la alerta establecida por el Gobierno Federal.
- Para comprobar la funcionalidad y experiencia en el uso de este esquema de trabajo, se opera aproximadamente una vez por mes (2011).
- La infraestructura utilizada para acceder al Banco, normalmente se encuentra bloqueada y se preestablecen fechas para operar bajo este esquema.

3. Falla de software en las ETB por contaminación de virus informático

- Para cubrir el escenario, se implementó la infraestructura siguiente:
  - A nivel Institucional, se instalaron *firewall's* y un sistema de control, que permite la ejecución de aplicaciones sobre la red de cómputo y telecomunicaciones del Banco, siempre y cuando estén registradas en el sistema de seguridad de informática.
  - Adicionalmente en la DGOBC, se instalaron de manera paralela, una red de seis terminales que utilizan como plataforma primaria el sistema operativo Unix diferente al estándar Microsoft utilizado en el Banco.
  - Unix proporciona a cada terminal su propio firewall y atrás de éste, se instala una ETB virtual limitando los servicios como el acceso a Internet o correo electrónico, para evitar una posible contaminación.
- Estas terminales se encuentran en las instalaciones primarias de operación de la DGOBC cubriendo el 49% de las aplicaciones a cargo de la GDSO.
- Para comprobar su funcionalidad, se opera en este tipo de terminales al menos 3 veces al año.

3. Falla de software en las ETB por contaminación de virus informático



4. Falla de servidores primarios

- Para cubrir este escenario, se cuenta con servidores alternos y procedimientos que permiten en general:
  - Replicar en línea y/o respaldar la información de la operación, en al menos un servidor alterno.
  - Trasladar la operación a servidores alternos, y
  - Reanudar el servicio en el servidor primario, al corregirse la falla y en la fecha que se determine.

- A partir de 2001, se realizan pruebas para operar las aplicaciones críticas en los servidores alternos, al menos una vez al año

5. Interrupción prolongada de una aplicación informática

- Para cubrir este escenario, las áreas operativas están armando sus Planes de Continuidad de Operativa (PCO) por aplicación informática
- Actualmente existen nueve planes de 45 aplicaciones (20%).
- Por cada nuevo PCO es necesario:
  - Que las áreas operativas contemplen el uso de procesos alternos o manuales, para continuar con su operación, ejemplo: uso del servicio telefónico, fax, archivos planos o de Excel, email, correspondencia, otros.
  - Que cuenten con un Plan de Recuperación para que el proceso o servicio interrumpido, recupere el estado normal de trabajo como si nada hubiera pasado.
  - Que sean probados y revisados regularmente.

Mantenimiento de la infraestructura

- Inmuebles
  - Supervisión de los servicios de apoyo: aire acondicionado, limpieza, accesos, letreros, seguridad, otros servicios.
- Reasignación de personal o cambio de rol (Clave, con Laptop)
  - Personalizar sus equipos, entrenar al personal, actualizar información.
- Nuevas aplicaciones, versiones o software
  - ETBs en el SOA, ETL y Laptops.
- Cambios de estructura, infraestructura, actualizaciones de NAI
  - Actualización directorios, croquis de trabajo, configuración de perfiles, creación de manuales de uso, supervisión y/o cambio de equipos.
- Pruebas de escenarios
  - Plan, supervisión, apoyo durante el ejercicio, recopilación y resumen de informes, seguimiento y/o resolución de problemas, mejora de procedimientos, acuerdos con proveedores de servicios.

Qué sigue

- Continuar manteniendo la infraestructura para la CO
- Seguir practicando

- Afinar los procesos críticos y los de apoyo
- Completar los PCO de los procesos críticos

- Compararnos con la BS25999 (cuantos «debes» cumplimos y cuantos nos faltan)
- Crear los planes que faltan - planes de cada escenario
- Revisar el análisis de impacto del negocio (AIN)

Lecciones aprendidas

- Información
  - Semáforo de alerta
  - Trípticos y Página Web
  - Compendio de Documentos
- Normatividad
  - Entre mayor nivel tenga quién impulsa la CO mayor será la cultura de CO
  - Clasificación de los procesos - críticos y de apoyo
  - Los procesos críticos deben tener su PCN
  - Clasificación del personal - crítico, suplente y de apoyo
- Infraestructura actualizada
  - Debe haber personal dedicado a la CO
  - El personal de CO debe ser enterado de los cambios en el negocio
  - Facilidades para los usuarios: ruteo de teléfonos (mismo tipo), correo, red
  - Procedimientos para reemplazo de tokens generadores de claves de acceso
- Entrenamiento constante
  - Pruebas periódicas lo más cercano a la realidad

Anexo 7

Procedimiento del Departamento de Informática del Ministerio de Trabajo y desarrollo Laboral (formato pdf)

República de Panamá

Ministerio de Trabajo y Desarrollo Laboral

RESOLUCION Nº DM/7 2011 **de** 14 de Enero **de 2011**

LA MINISTRA DE TRABAJO Y DESARROLLO LABORAL
En uso de su facultades legales, que le confiere la Ley,

CONSIDERANDO:

Que el Ministerio de Trabajo y Desarrollo Laboral, como parte integral del Gobierno Central, actualmente esta realizando acciones encaminadas a agilizar y simplificar trámites, para mejorar el proceso de modernización institucional y la gestión administrativa de la Institución.

Que el Decreto Ejecutivo No 249 de 16 de julio de 1970, faculta al Ministerio de Trabajo y Desarrollo Laboral, para que dentro de sus atribuciones y responsabilidades administrativas, pueda crear, eliminar, reformar y/o reorganizar la estructura organizativa de la Institución a su cargo.

Que la Dirección de Planificación, a través del Departamento de Planificación Institucional, ha analizado procesos para organizar y sistematizar el flujo de la información aplicando en forma extensiva los métodos que ayuden a la tecnificación de las funciones, con ese propósito ha elaborado "El Manual de Procedimientos de la Unidad de Informática" con sus respectivos formularios.

RESUELVE:

ARTICULO PRIMERO: Aprobar el Manual de Procedimientos de la Unidad de Informática con sus formularios, que se utilizarán en esa dependencia de la Dirección de Administración y Finanzas.

ARTICULO SEGUNDO: Autorizar a la Dirección de Planificación para que, en la medida que sea necesario, actualice el Manual de Procedimiento de la Unidad de Informática y sus formularios, con el objeto de incorporar técnicas o cambios para mejorar la gestión institucional.

PUBLÍQUESE Y CÚMPLASE

ALMA LORENA CORTÉS A.
Ministra de Trabajo y Desarrollo Laboral

LUIS ERNESTO CARLES
Viceministro de Trabajo y Desarrollo Laboral

MINISTERIO DE TRABAJO Y DESARROLLO LABORAL

DESPACHO SUPERIOR

ALMA LORENA CORTÉS A.
Ministra

LUIS ERNESTO CARLES R.
Viceministro

HERNÁN GARCÍA APARICIO
Secretario General

RUBÉN DARÍO CAMPOS
Director de Planificación

MINISTERIO DE TRABAJO Y DESARROLLO LABORAL

EQUIPO TÉCNICO DE APOYO

DIRECCIÓN DE PLANIFICACIÓN

DEPARTAMENTO DE PLANIFICACIÓN INSTITUCIONAL

MANUEL RODRÍGUEZ
Jefe del Departamento de Planificación Institucional

KIREM FORERO
Analista de Organizaciones y Sistemas

DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS

SAMUEL BELUCHE
Director Administrativo

MARÍA DEL CARMEN MIRANDA
Jefa de la Unidad de Informática

MINISTERIO DE TRABAJO Y DESARROLLO LABORAL
MANUAL DE PROCEDIMIENTO DE LA UNIDAD DE INFORMÁTICA

INTRODUCCIÓN

La Dirección de Planificación a través del Departamento de Planificación Institucional, lleva a cabo análisis de procedimientos para la agilización de trámites administrativos.

Los Manuales de procedimientos son instrumentos que apoyan el quehacer diario de las instituciones y son considerados herramientas fundamentales para la coordinación, dirección, evaluación y el control administrativo, así como para consulta en el desarrollo cotidiano de actividades.

El Manual de Procedimiento de la Unidad de Informática se ha elaborado, con el objeto de integrar procedimientos de reportes de las necesidades en cuanto al sistema de cómputo, dentro y en cada una de las regionales del Ministerio de Trabajo y Desarrollo Laboral.

Esperamos que este manual sea un instrumento de orientación al personal que labora en esta unidad administrativa, coadyuvando asi a mejorar el servicio.

Estos procedimientos son flexibles por consiguientes estamos anuentes a considerar las recomendaciones que surjan de su aplicación por lo que, cualquiera aportación sobre la materia, se recomienda comunicarla y fundamentarla por escrito a la Dirección de Planificación, quien es responsable de esta labor.

MINISTERIO DE TRABAJO Y DESARROLLO LABORAL
MANUAL DE PROCEDIMIENTO DE LA UNIDAD DE INFORMÁTICA

ÍNDICE

MINISTERIO DE TRABAJO Y DESARROLLO LABORAL
MANUAL DE PROCEDIMIENTO DE LA UNIDAD DE INFORMÁTICA

I. ASPECTOS GENERALES

A Objetivos:

Establecer las acciones a tomar para organizar y sistematizar el flujo de la información de la Unidad de Informática, aplicando en forma extensiva los métodos que ayuden a la tecnificación de las funciones y procedimientos que se realizan en las distintas instancias

B. Marco Legal:

Decreto de Gabinete No 2 de 15 de enero de 1969. Por medio del cual se crea el Ministerio de Trabajo y Bienestar Social y se asignan funciones

Decreto Nº 249 de 16 de julio de 1970. Por el cual se dicta la Ley Orgánica del Ministerio de Trabajo y Bienestar Social,

Decreto de Gabinete Nº 252 de 30 de diciembre de 1971. Por el cual se aprueba el Código de Trabajo.

Decreto Ejecutivo No 2 de 8 de febrero de 1991. Por el cual se adoptan algunas disposiciones y medidas sobre la organización del Ministerio de Trabajo y Bienestar Social, en su artículo 2 señala la creación de la Unidad de Apoyo Sistema de Informática.

El Decreto Ejecutivo Nº 17 de 18 de abril de 1994. Por el cual se aprueba el Reglamento Orgánico del Ministerio de Trabajo y Bienestar Social.

Ley Nº 42 del 19 de noviembre de 1997, Por el cual se crea el Ministerio de la Juventud, la Mujer, la Niñez y la Familia, en su artículo 28 señala la nueva denominación del Ministerio de Trabajo y Desarrollo Laboral.

Resolución No D M 118 – 2010 de 7 de abril de 2010. Por el cual se crea el comité interdisciplinario encargado de dar seguimiento a la actualización de la información en la página Web del Ministerio de Trabajo y Desarrollo Laboral.

C. Alcance del Manual

Establecer un conjunto de normas y procedimientos, para que la Unidad de Informática del Ministerio de Trabajo y Desarrollo Laboral tenga la responsabilidad de identificar, formular, establecer y administrar todo lo referente al sistema de informática.

D. Responsabilidad

La Unidad de Informática que pertenece a La Dirección de Administración y Finanzas, es la responsable de identificar el apoyo que requieran del sistema de informática, recolección de datos, mantener registros y archivos actualizados, establecer redes de comunicación a nivel interno, orientar a usuarios sobre las normas de los sistemas implantados, desarrollar bases de datos en áreas que lo requieran y las de mas funciones inherentes en el sistema

E. Definición.

Informática:

Informática es la ciencia aplicada que abarca el estudio y aplicación del tratamiento automático de la información, utilizando dispositivos electrónicos y sistemas computacionales. También está definida como el procesamiento automático de la información.

F. Unidad de Informática

Objetivo:

Organizar y sistematizar el flujo de la información de la unidad de información de la institución, aplicando en forma extensiva los métodos que ayuden a la tecnificación de las funciones y procedimientos que se realizan en las distintas instancias.

Tendrá las siguientes funciones:

- Identificar las dependencias del ministerio que requieran del apoyo del Sistema de Informática, para potenciar su acción.
- Formular y realizar un plan de recolección de datos que contenga un sistema integrado de la información proveniente de las distintas instancias del ministerio.
- Mantener registros y archivos electrónicos actualizados y que alimenten el banco de datos socio-laborales.
- Instrumentar sistemas electrónicos mediante programas o paquetes de información procesamiento y control.

- Posibilitar el manejo de herramientas de análisis estadísticos de la información estableciendo redes de comunicación a nivel interno.
- Establecer canales de comunicación con el resto del sistema de información nacional.
- Elaborar manuales de operación para el proceso de los sistemas.
- Orientar a los usuarios respecto a las normas que rigen los sistemas implantados.
- Ejecutar el programa de automatización desarrollando bases de datos y aplicaciones en las áreas que lo requiera,
- Administrar los recursos computacionales para asegurar el mejor aprovechamiento de estos.
- Ejercer las demás funciones inherentes al sistema.
- Mantener registros de la labor efectuada en la unidad.

II. PROCEDIMIENTOS

A. SOLICITUD DE SOPORTE TÉCNICO

DIRECCIONES, DEPARTAMENTOS Y SECCIONES

SOLICITANTE

El solicitante de la direcciones, departamentos y secciones del Ministerio de Trabajo y Desarrollo Laboral mediante una llamada telefónica (Ext 1067), nota interna o vía correo electrónico a la recepcionista solicita que requiere el servicio de la Unidad de Informática.

UNIDAD DE INFORMÁTICA

RECEPCIONISTA

La recepcionista ingresa a MANTIS y reporta la incidencia, se le asigna al técnico y MANTIS le envía un correo electrónico indicándole que tiene un soporte.

La recepcionista imprime el soporte el técnico lo retira en la recepción.

TÉCNICO

El técnico recibe el reporte y se dirige a la unidad solicitante, verifica el problema y lo resuelve.

Si el técnico no puede resolver el problema, entonces debe ingresar al MANTIS y hacer una de las dos (2) opciones; asignarle el soporte a otra persona o seleccionar si necesitan más datos. En éste último caso el administrador debe asignar nuevamente el soporte.

DIRECCIONES, DEPARTAMENTOS Y SECCIONES

SOLICITANTE

Una vez reparado o no el problema, la persona solicitante debe firmar el reporte presentado por el técnico anotando el nombre, fecha y hora de la reparación como constancia de que se realizo el soporte.

UNIDAD DE INFORMÁTICA

TÉCNICO

Cuando el técnico regresa a la Unidad de Informática, le entrega el reporte a la recepcionista.

El técnico ingresa al MANTIS, documentando lo que realizó y la solución, debe colocar la incidencia como resuelta.

RECEPCIONISTA

La recepcionista recibe un correo electrónico de MANTIS indicando que la incidencia fue resuelta; la recepcionista procede a llamar al usuario que solicitó el soporte para validar que fue efectivamente atendido, y con esta información procede a cerrar la incidencia en el MANTIS.

JEFA/E

A final de mes, se obtienen las estadísticas de los soportes técnicos realizados a las direcciones, departamentos y secciones del MITRADEL.

Se detalla los soportes realizados de las direcciones, departamentos y secciones que más solicitan soportes técnicos.

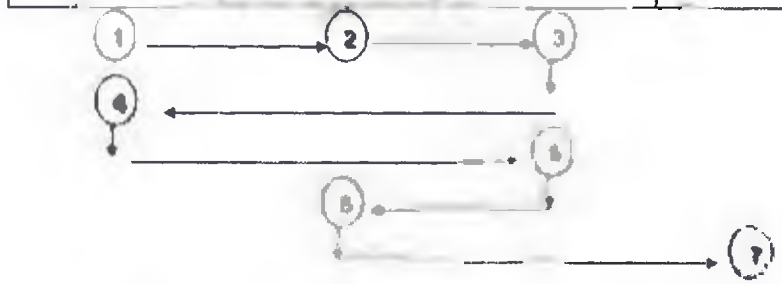
Estas estadísticas son presentadas al despacho del Ministerio de Trabajo y Desarrollo Laboral y a la Dirección de Administración y Finanzas.

MINISTERIO DE TRABAJO Y DESARROLLO LABORAL
MANUAL DE PROCEDIMIENTO DE LA UNIDAD DE INFORMÁTICA

A SOLICITUD DE SOPORTE TÉCNICO

MAPEO
MINISTERIO DE TRABAJO Y DESARROLLO LABORAL

DIRECCIÓN	DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS			
DEPARTAMENTO				
SECCIÓN	UNIDAD DE INFORMÁTICA			
SOLICITANTE	RECEPCIONISTA	TÉCNICO	JEFA	



DESCRIPCIÓN DEL PROCESO

1	El solicitante mediante una llamada telefónica, nota interna o correo electrónico a la recepcionista solicita soporte técnico a la Unidad de Informática.
2	La recepcionista recibe las llamadas o las solicitudes escritas que requieren el servicio. Esta a su lo ingresa a MANTIS, lo imprime y entrega al técnico.
3	El técnico recibe el reporte y se dirige a la unidad solicitante para la verificación, reparación del equipo.
4	Una vez reparado la persona solicitante debe firmar el reporte presentado por el técnico anotando el nombre, fecha y hora como constancia de que se realizo la reparación.
5	El técnico ingresa al MANTIS el soporte técnico y lo envia a la recepcionista por correo electrónico para cerrar el soporte técnico
6	La recepcionista recibe un correo electrónico de MANTIS indicando que la incidencia fue resuelta; la recepcionista procede a llamar al usuario que solicitó el soporte para validar que fue efectivamente atendido, con esta información procede a cerrar la incidencia en el MANTIS.
7	El Jefe/a de la Unidad de Informática a fin de mes, presenta informe de los soportes técnicos más solicitados por las direcciones, departamento y secciones al despacho del ministro y a la Dirección de Administración y Finanzas.

B. SOLICITUD DE SOPORTE TÉCNICO DE LAS REGIONALES

DIRECCIONES REGIONALES

SOLICITANTE

El solicitante de la Dirección Regional del Ministerio de Trabajo y Desarrollo Laboral mediante una nota o correo electrónico solicita soporte técnico a la Unidad de Informática.

UNIDAD DE INFORMÁTICA

JEFE (A)

El Jefe (a) autoriza la solicitud de la regional y da instrucciones a la recepcionista.

RECEPCIONISTA

La recepcionista ingresa el reporte en el sistema MANTIS donde registra nombre de la unidad, tipo de equipo, daño, nombre del técnico que realizará la reparación e iniciar los trámites de los viáticos a fin de hacer efectiva la gira.

TÉCNICO

El técnico realiza las reparaciones en la regional de trabajo; entrega al director o personal responsable el formulario de visita a las regionales donde se registra los problemas encontrados y sus respectivas soluciones como constancia de la visita.

El técnico cuando llega a la Unidad de Informática, presenta un informe detallado de los trabajos realizados a la Jefa de la Unidad de Informática.

DIRECCION REGIONAL

SOLICITANTE

Una vez realizado el soporte técnico el director regional o la persona encargada firma el formulario presentado por el técnico anotando el nombre (firma) como constancia de que se realizo la reparación.

MINISTERIO DE TRABAJO Y DESARROLLO LABORAL
MANUAL DE PROCEDIMIENTO DE LA UNIDAD DE INFORMÁTICA

B. SOLICITUD DE SOPORTE TÉCNICO DE LAS REGIONALES

MAPEO

DESCRIPCIÓN DEL PROCESO

1. El solicitante mediante una nota o correo electrónico solicita soporte técnico a la Unidad de Informática.
2. El Jefe (a) autoriza la solicitud de la regional y da instrucciones a la recepcionista.
3. La recepcionista ingresa el reporte en el sistema MANTIS, donde registra nombre de la unidad, tipo de equipo, daño, nombre del técnico que realizará la reparación.
4. El técnico recibe el reporte y se dirige a la regional en el dia programado para realizar la reparación; cuando el técnico llega a la sede principal del MITRADEL, presenta un informe detallado a la Jefa de la Unidad de Informática.
5. Una vez realizado el soporte técnico, el director regional o la persona encargada firma el reporte de "visita a las Regionales", presentado por el técnico.

C. ACCESO FÍSICO A LA UNIDAD DE INFORMATICA Y ÁREAS RESTRINGIDAS

Las normas para seguridad física brindan el marco para evitar acceso no autorizado, daños e interferencias en la información del Ministerio de Trabajo y Desarrollo Laboral.

Los funcionarios de la Unidad de Informática tienen su entrada controlada por medio de una tarjeta electrónica.

VISITANTE

Los visitantes que ingresen a la Unidad de Informática tienen que registrase en la recepción firmando la entrada.

La entrada de cualquiera persona al data center dentro y fuera del horario habitual de trabajo, deberá estar autorizado formalmente y registrada en la bitácora de la recepción por el Jefe, Subjefe o Administrador de Seguridad.

UNIDAD DE INFORMÁTICA

RECEPCIONISTA

La recepcionista registra al visitante y notifica al Jefe (a) de la Unidad de Informática de la presencia de una visita.

JEFE (A)

El Jefe (a) acompañará a la visita o asignará a un funcionario para que lo escolte a las diferentes secciones de la unidad.

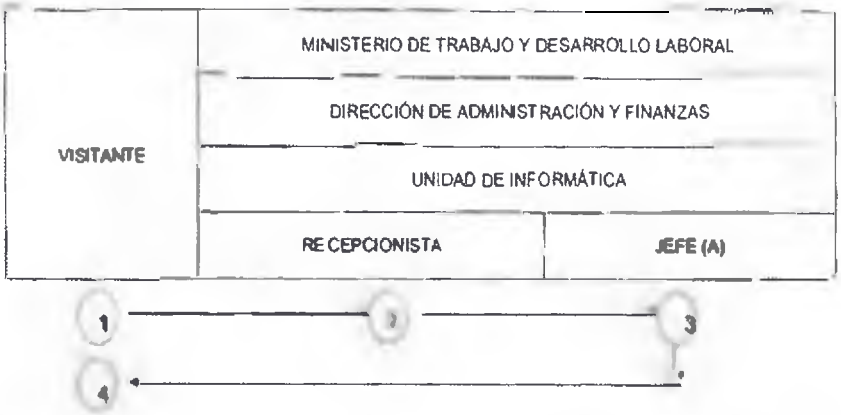
VISITANTE

La visita se retira firmando el registro en la parte de salida.

MINISTERIO DE TRABAJO Y DESARROLLO LABORAL
MANUAL DE PROCEDIMIENTO DE LA UNIDAD DE INFORMÁTICA

C) ACCESO FÍSICO A LA UNIDAD DE INFORMATICA Y AREAS RESTRINGIDAS

MAPEO



DESCRIPCIÓN DEL PROCESO

1	Los visitantes que ingresen a la Unidad de Informática tienen que registrarse en la recepción firmando la entrada.
2	La recepcionista registra al visitante y notifica al Jefe (a) de la Unidad de Informática de la presencia de una visita.
3	El Jefe (a) acompañará a la visita o asignará a un funcionario para que lo escolte a las diferentes secciones de la unidad.
4	La visita se retira firmando el registro en la parte de salida.

D. ACTUALIZACIÓN DE LA APLICACIÓN SIAFPA

El Ministerio de Economía y Finanzas, a través de la Dirección Nacional de Contabilidad, crea la Dirección Nacional del Sistema Integrado de Administración Financiera de Panamá, que son los responsables de la organización, dirección y control de los procesos y recursos compartidos de los sistemas de información automatizados de la administración financiera de Panamá.

El Sistema Integrado de Administración Financiera de Panamá (SIAFPA) está conformado por los módulos de presupuesto, tesorería, deuda pública y contabilidad.

La aplicación SIAFPA requiere una actualización periódica. Muchas veces esta actualización afecta sólo proceso de un área determinada. Por ejemplo, los procesos de contabilidad. En este caso solo se requiere actualizar los equipos de contabilidad.

UNIDAD DE INFORMÁTICA

TÉCNICO

El personal de informática solicita la contraseña y es el único responsable de ingresar a la página del Ministerio de Economía y Finanzas para descargar las actualizaciones.

Estas actualizaciones se realizan en las computadoras clientes a Siafpa, se actualizan cada vez que exista una nueva actualización.

MINISTERIO DE ECONOMÍA Y FINANZAS

DIRECCIÓN NACIONAL DE CONTABILIDAD SIAFPA

La dirección de base de datos de SIAFPA suministra la contraseña de los archivos comprimidos a la Unidad de Informática para realizar las actualizaciones.

UNIDAD DE INFORMÁTICA

TÉCNICO

Realiza las actualizaciones.

MINISTERIO DE TRABAJO Y DESARROLLO LABORAL
MANUAL DE PROCEDIMIENTO DE LA UNIDAD DE INFORMÁTICA

D. ACTUALIZACIÓN DE LA APLICACIÓN SIAFPA

MAPEO

MINISTERIO DE TRABAJO Y DESARROLLO LABORAL	MINISTERIO DE ECONOMÍA Y FINANZAS
DIRECIÓN DE ADMINISTRACIÓN FINANZAS UNIDAD DE INFORMÁTICA	DIRECCIÓN NACIONAL DE CONTABILIDAD SIAFPA
TÉCNICO	

DESCRIPCIÓN DEL PROCESO

1	El personal de informática solicita la contraseña y es el único responsable de ingresar a la página del Ministerio de Economía y Finanzas para descargar las actualizaciones.
2	La dirección de base de datos de SIAFPA suministra la contraseña de los archivos comprimidos a la Unidad de Informática para realizar las actualizaciones.
3	Realiza las actualizaciones.

E. SOLICITAR PERMISO DE USUARIO

El Ministerio de Trabajo y Desarrollo Laboral, se realizan diversas tareas en las que se requieren que el personal tenga usuario para realizar las mismas.

Estos usuarios son usuarios de red, usuarios de correo electrónico, y usuarios de aplicaciones.

USUARIO

La solicitud de usuario se realiza por el Jefe directamente a la Dirección de Administración y Finanzas a través de correo electrónico dirigido al director con copia a la Unidad de Informática.

DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS

DIRECTOR

El Director de Administración y Finanzas aprueba la solicitud, la nota es reenviada a la Unidad de Informática para que ejecute la solicitud.

UNIDAD DE INFORMÁTICA

JEFE

La solicitud de usuario llega al Jefe (a) de la Unidad de Informática donde a su vez es reenviado a la recepción para que sea ingresado al sistema MANTIS donde se asigna al técnico encargado de proceder a la solicitud.

TÉCNICO

Recibe la solicitud y procede a crear el usuario y le notifica

USUARIO

Recibe el correo electrónico y procede a ingresar al sistema, correo electrónico o red.

OBSERVACIÓN:

- Si la solicitud es para usuario de red, se le asigna al técnico responsable (técnico administrador de seguridad).

- Si la solicitud es para permiso de correo electrónico, se le envía al técnico administrador de red.

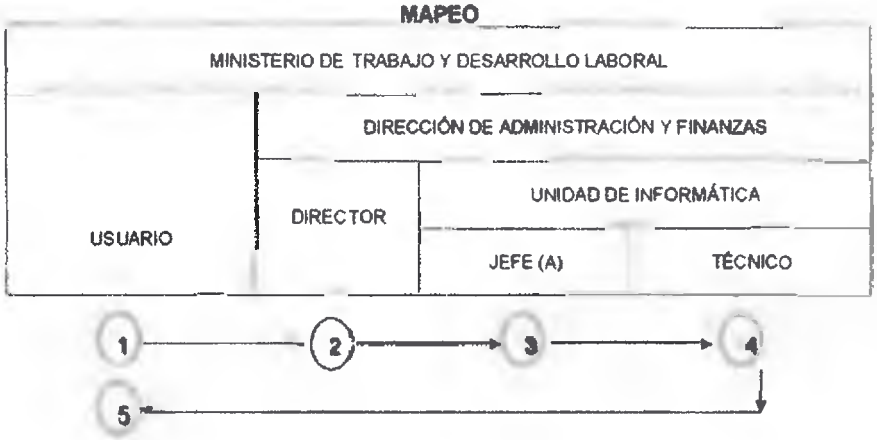
- Si la solicitud es para usuario de aplicaciones, se le envía al técnico administrador de base de datos.

Una vez que cada técnico crea los usuarios, éste los ingresa al sistema MANTIS. La Recepcionista llama a la unidad solicitante para proporcionarle su usuario y contraseña.

MINISTERIO DE TRABAJO Y DESARROLLO LABORAL
MANUAL DE PROCEDIMIENTO DE LA UNIDAD DE INFORMÁTICA

I. SOLICITAR PERMISO DE USUARIO

MAPEO



DESCRIPCIÓN DEL PROCESO

1	Solicita a la Dirección de Administración y Finanzas permiso correspondiente para un nuevo usuario.
2	El Director de Administración y Finanzas con previa autorización, reenvía solicitud a la Unidad de Informática.
3	El Jefe (a) de la Unidad de Informática remite correo electrónico a la recepcionista para que ésta a su vez lo ingrese en el sistema MANTIS la solicitud de usuario.
4	El técnico asignado, se apersona a la unidad solicitante donde procede a efectuar la instalación de usuario.
5	Una vez terminado la instalación el técnico entrega pro forma donde el usuario firma como constancia de que el trabajo fue realizado.

III FORMULARIOS

MINISTERIO DE TRABAJO Y DESARROLLO LABORAL
MANUAL DE PROCEDIMIENTO DE LA UNIDAD DE INFORMÁTICA

SISTEMA MANTIS

A. OBJETIVO:

Llevar un control de las necesidades en base a la demanda de nuestros usuarios en lo concerniente a: mantenimiento y reparación de equipos, instalación de software y hardware, cableado estructurado y de telefonía, configuración de la red y telecomunicaciones.

B. ORIGEN:

Unidad de Informática.

C. CONTENIDO:

1	ID	Número de la identificación del soporte
2	Categoria	Indicar el nombre del Enlace que envía la información
3	Severidad	Señalar el nombre de la Dirección, Departamento o Sección que envía la información
4	Reproducibilidad	Escribir brevemente de que se trata la información enviada
5	Fecha de envió	Anotar con un gancho si se publica o no.
6	Ultima Actualización	Indicar la fecha que se publica la información
7	Informador	Persona que hace el reporte o la incidencia
8	Asignado a	al Técnico de la Unidad de Informática
9	Prioridad	Si es un soporte normal, urgente, etc.
19	Resolución	
20	Resumen	Nombre del usuano que solicitó el soporte.
21	Descripción	Detalle del problema que tiene el equipo
25	Fecha de Modificación	Se registra las fechas cada vez que se hacen arreglos al equipo de cómputo asignado.
26	Usuario	Se refiere al Técnico o Administrador asignado para esta tarea.
27	Campo	Se refiere a lo que se notificó a la unidad de informática.
28	Cambio	Se refiere a quien se le asignó o cuales fueron los cambios efectuados al equipo.

*Hacemos la observación que los técnicos de la Unidad de Informática no llenan todo el formulario ya que solo anotan lo primordial en el mantis.

MINISTERIO DE TRABAJO Y DESARROLLO LABORAL
MANUAL DE PROCEDIMIENTO DE LA UNIDAD DE INFORMÁTICA

ANEXO No 1

SISTEMA MANTIS

Vista Avanzada de la Incidencia

ID:	Categoría:	Severidad:	Reproducibilidad:	fecha de envió:	Última Actualización:
1	2	3	4	5	6

Informador:	7	Plataforma:	13
Asignado a:	8	Sistema:	14
Prioridad:	9	Operativo:	15
Estado:	10	Versión de S.O.:	16
Compilación del Producto:	11	Versión del Producto:	17
Proyección Tiempo Estimado:	12	Resolución:	18
		Resuelto en Versión:	19

Resumen:	20
Descripción:	21
Pasos para reproducirlo:	22
Información Adicional:	23
Relaciones	
Archivos Adjunto:	24

Historial de La incidencia

Fecha de Modificación	Usuario	Campo	Cambio
25	26	27	28

MINISTERIO DE TRABAJO Y DESARROLLO LABORAL
MANUAL DE PROCEDIMIENTO DE LA UNIDAD DE INFORMÁTICA

VISITA A LAS REGIONALES DE TRABAJO

A. OBJETIVO:

Llevar un control de los problemas encontrados y solucionados en cada una de las Regionales de Trabajo.

B. ORIGEN:

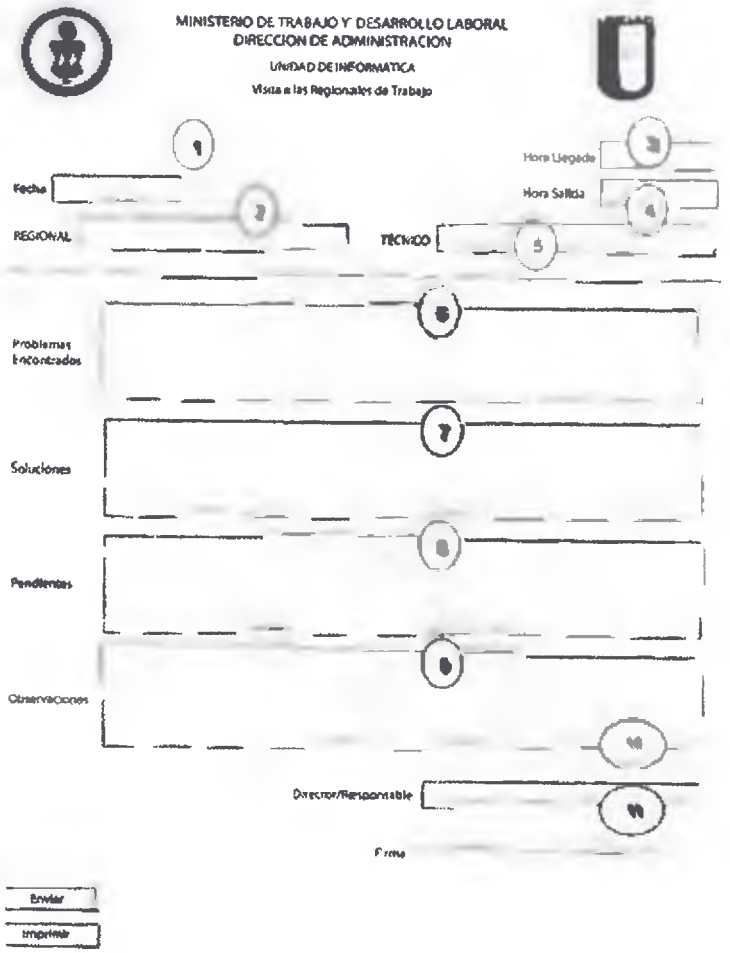
Regionales del Ministerio de Trabajo y Desarrollo Laboral

C. CONTENIDO:

1. Fecha	Se anota la fecha en que el técnico de la unidad de informática realiza el soporte técnico.
2. Regional:	Se anota la Regional que solicita el apoyo técnico.
3. Hora de Llegada:	Se anota la hora en que llega el Técnico de la Unidad de Informática.
4. Hora de Salida:	Se anota la hora de salida del Técnico de la Unidad de Informática
5. Técnico:	Nombre del Técnico de la Unidad de Informática asignado.
6. Problemas Encontrados:	Se anota las anomalías encontradas en el equipo reportado.
7. Soluciones:	Se detalla lo que se hizo, lo que se pudo resolver.
8. Pendientes:	Se detalla lo que quedó pendiente del trabajo asignado.
9. Observaciones:	Se detalla si hay alguna observación relevante en cuanto a la reparación del equipo asignado.
10: Director / Responsable:	Se anota el nombre del Director o persona responsable del equipo en reparación.
11: Firma:	Se anota la firma del Director o persona responsable.

MINISTERIO DE TRABAJO Y DESARROLLO LABORAL
MANUAL DE PROCEDIMIENTO DE LA UNIDAD DE INFORMÁTICA

ANEXO No 2



Anexo 8

Situación Actual del Data Center del Ministerio de Trabajo y Desarrollo Laboral